This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
# Table of Contents

## Preface

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>ix</td>
</tr>
<tr>
<td>Document Set</td>
<td>x</td>
</tr>
<tr>
<td>Intended Audience</td>
<td>x</td>
</tr>
<tr>
<td>Document Conventions</td>
<td>xi</td>
</tr>
<tr>
<td>About Trend Micro</td>
<td>xii</td>
</tr>
</tbody>
</table>

## Part I: Endpoint Encryption Overview

### Chapter 1: Introducing Endpoint Encryption

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Endpoint Encryption</td>
<td>1-2</td>
</tr>
<tr>
<td>Key Features and Benefits</td>
<td>1-2</td>
</tr>
<tr>
<td>What's New in Version 5.0</td>
<td>1-3</td>
</tr>
<tr>
<td>About Encryption</td>
<td>1-6</td>
</tr>
<tr>
<td>Endpoint Encryption Components</td>
<td>1-7</td>
</tr>
</tbody>
</table>

### Chapter 2: Devices and Users Overview

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Encryption Devices</td>
<td>2-2</td>
</tr>
<tr>
<td>Endpoint Encryption Users</td>
<td>2-4</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>2-6</td>
</tr>
</tbody>
</table>

## Part II: Administration with Trend Micro Control Manager

### Chapter 3: Getting Started with Control Manager

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Control Manager Integration</td>
<td>3-2</td>
</tr>
</tbody>
</table>
Control Manager Architecture ............................................................... 3-3
Configuring Control Manager Summary of Operations ....................... 3-6
Adding PolicyServer as a Managed Product to Control Manager .......... 3-7
Configuring Directory Management for PolicyServer ....................... 3-9
Creating a Policy .................................................................................. 3-10

Chapter 4: Dashboard, Widgets, and Reports
Using the Dashboard ............................................................................. 4-2
Understanding Tabs .............................................................................. 4-2
Understanding Widgets ....................................................................... 4-4
Using Endpoint Encryption Widgets .................................................... 4-8

Chapter 5: Policies in Control Manager
Groups .................................................................................................. 5-2
Understanding Policies ......................................................................... 5-2
Understanding Policy Types ................................................................. 5-3
Understanding Policy Target Settings .................................................. 5-6
Understanding the Policy List ............................................................... 5-6
Understanding the Managed Server List ............................................. 5-26
Updating the Policy Templates ............................................................. 5-31

Chapter 6: Users in Control Manager
Endpoint Encryption Users Widget ....................................................... 6-3
Adding Users to Endpoint Encryption .................................................. 6-4
Finding a User ..................................................................................... 6-10
Modifying a User .................................................................................. 6-10
Working with Passwords ................................................................. 6-11
Working with Policy Membership ..................................................... 6-16
Chapter 7: Devices in Control Manager

Adding a Device to a Policy ................................................................. 7-3
Removing a Device From a Policy ...................................................... 7-6
Endpoint Encryption Devices Widget ............................................... 7-7
Finding a Device .............................................................................. 7-9
Getting a Software Token ............................................................... 7-9
Getting a Recovery Key ................................................................. 7-10
Viewing Device Attributes ............................................................... 7-11
Killing a Device .............................................................................. 7-14
Locking a Device ........................................................................... 7-15
Resetting a Device ....................................................................... 7-15
Deleting a Device From the Enterprise ......................................... 7-16
Restoring a Deleted Device ............................................................ 7-17

Part III: Administration with Endpoint Encryption PolicyServer MMC

Chapter 8: Getting Started with PolicyServer MMC

About PolicyServer MMC ................................................................. 8-2
Logging on to PolicyServer MMC .................................................. 8-2
PolicyServer MMC Interface .......................................................... 8-4
Working with Groups and Users .................................................... 8-5
Understanding Policy Controls ..................................................... 8-15
Disabling Agents .......................................................................... 8-19

Chapter 9: Policies in PolicyServer MMC

Policy Overview ............................................................................. 9-2
Automatic Policy Synchronization ............................................... 9-14
PolicyServer Policies ................................................................. 9-14
Full Disk Encryption Policies ..................................................... 9-19
File Encryption Policies ............................................................. 9-26
Common Policies ...................................................................... 9-30

Chapter 10: Groups in PolicyServer MMC
About Groups ........................................................................... 10-2
Group Management .................................................................... 10-2
Offline Groups .......................................................................... 10-12

Chapter 11: Users in PolicyServer MMC
Adding Users to Endpoint Encryption ........................................ 11-3
Finding a User ......................................................................... 11-8
Modifying a User ...................................................................... 11-9
Viewing a User's Group Membership ....................................... 11-10
Adding a New User to a Group ............................................... 11-11
Adding an Existing User to a Group ....................................... 11-13
Changing a User's Default Group .......................................... 11-15
Allowing User to Install to a Group ........................................... 11-16
Removing Users From a Group .............................................. 11-17
Removing All Users From a Group ......................................... 11-18
Restoring a Deleted User ....................................................... 11-18
Working with Passwords ....................................................... 11-19

Chapter 12: Devices in PolicyServer MMC
Adding a Device to a Group ...................................................... 12-3
Removing a Device from a Group ........................................... 12-4
Deleting a Device from the Enterprise .................................... 12-5
Getting the Software Token .................................................... 12-6
Using the Recovery Key .............................................................. 12-7
Viewing Device Attributes ...................................................... 12-8
Viewing Directory Listing ....................................................... 12-11
Viewing Group Membership ................................................... 12-11
Killing a Device .................................................................. 12-12
Locking a Device .................................................................. 12-12
Resetting a Device ............................................................. 12-13
Restoring a Deleted Device .................................................. 12-13

Part IV: Endpoint Encryption Agent Management

Chapter 13: File Encryption
About File Encryption ............................................................... 13-2
File Encryption Authentication .............................................. 13-2
File Encryption Agent Menu ................................................. 13-10
File Encryption Context Menu .............................................. 13-13
File Encryption Archive Encryption .................................... 13-14
File Encryption Archive and Burn ....................................... 13-18
File Encryption Secure Delete .............................................. 13-19

Chapter 14: Full Disk Encryption
About Full Disk Encryption ..................................................... 14-2
Endpoint Encryption Tools ..................................................... 14-2
Full Disk Encryption Preboot ................................................ 14-3
Full Disk Encryption Connectivity ...................................... 14-17
Full Disk Encryption Recovery Console .............................. 14-20
Full Disk Encryption Recovery Methods ............................................... 14-32
Repair CD .................................................................................................... 14-34
Patch Management with Full Disk Encryption ............................... 14-41

Chapter 15: Encryption Management for Third-Party Products

About Encryption Management Agents ................................................... 15-2
Encryption Management Agent Policy Limitations ......................... 15-3
Encryption Management for Microsoft BitLocker ............................... 15-4
Encryption Management for Apple FileVault ...................................... 15-10

Part V: Advanced Management and Technical Support

Chapter 16: Advanced Enterprise Features

Enterprise Maintenance ................................................................. 16-2
Restoring Deleted Users and Devices .............................................. 16-10
Enterprise Log Events ................................................................. 16-11
Enterprise Reports .......................................................................... 16-15

Chapter 17: Maintenance and Technical Support

Maintenance Agreement ................................................................. 17-2
Troubleshooting Resources ............................................................ 17-5
Contacting Trend Micro ............................................................... 17-7
Other Resources .............................................................................. 17-8

Appendices

Appendix A: Introducing Trend Micro Control Manager
Control Manager Standard and Advanced ................................................. A-3
Introducing Control Manager Features ...................................................... A-3
Control Manager Architecture ..................................................................... A-5
Registering Endpoint Encryption to Control Manager ........................... A-8
Understanding User Access ................................................................. A-9
Understanding the Product Directory .................................................. A-15
Downloading and Deploying New Components ................................... A-38
Using Logs .................................................................................................... A-65
Understanding Reports ............................................................................... A-68

Appendix B: PolicyServer Message IDs

Appendix C: Endpoint Encryption Services

Appendix D: Policy Mapping Between Management Consoles

Appendix E: OfficeScan Integration

  About Trend Micro OfficeScan Integration ............................................. E-2
  About Plug-in Manager .......................................................................... E-3
  Installing OfficeScan ............................................................................. E-4
  Using Plug-in Programs ......................................................................... E-5
  The OfficeScan Agent Tree ..................................................................... E-5
  Endpoint Encryption Agent Deployment ............................................. E-9

Appendix F: Glossary

Index

  Index .............................................................................................................. IN-1
Welcome to the Trend Micro™ Endpoint Encryption™ Administrator's Guide. This guide explains the security architecture, management console options, user authentication, and endpoint management. This guide also describes how to configure the management consoles and Endpoint Encryption agents to support security objectives, how to provision Endpoint Encryption users, groups and devices to implement policies, how to use reports and logs to analyze enterprise security, and includes information about troubleshooting configurations, using tools, and resolving issues.

Topics include:

• **Document Set on page x**
• **Intended Audience on page x**
• **Document Conventions on page xi**
• **About Trend Micro on page xii**
Document Set

The documentation set for Trend Micro Endpoint Encryption includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Help</td>
<td>All products contain an entry point to access the online help. The online help provides access the context-sensitive HTML help topics.</td>
</tr>
<tr>
<td>Readme File</td>
<td>Contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

Intended Audience

This guide is for IT Administrators deploying Trend Micro Endpoint Encryption in medium to large enterprises and Help Desk personnel who manage users, groups, policies, and devices. The documentation assumes basic device, networking and security knowledge, including:

- Endpoint hardware setup and configuration
• Basic endpoint encryption concepts
• Hard drive partitioning, formatting, and maintenance
• Client-server architecture

Document Conventions

The documentation uses the following conventions:

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>References to other documents</td>
</tr>
<tr>
<td>Monospace</td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
</tbody>
</table>
About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.
Part I

Endpoint Encryption Overview
Chapter 1

Introducing Endpoint Encryption

This chapter introduces Endpoint Encryption features and capabilities.

Topics include:

•  About Endpoint Encryption on page 1-2
•  Key Features and Benefits on page 1-2
•  What's New in Version 5.0 on page 1-3
•  About Encryption on page 1-6
•  Endpoint Encryption Components on page 1-7
About Endpoint Encryption

Trend Micro Endpoint Encryption ensures privacy by encrypting data stored on endpoints, files and folders, and removable media in a variety of platform options. Endpoint Encryption provides granular policy controls and flexibly integrates with other Trend Micro management tools, including Control Manager and OfficeScan. Innovative deployment capabilities help you easily deploy agent software using FIPS 140-2 hardware-based or software-based encryption that is fully transparent to end users, without disrupting productivity. Once deployed, automated reporting, auditing, and policy synchronization with Endpoint Encryption PolicyServer simplifies endpoint security management.

Endpoint Encryption has capabilities to deploy remote commands, recover lost data, and protect user identity while maintaining real-time policy synchronization. In the event that an endpoint is lost or stolen, remotely initiate a reset or “kill” command to immediately protect corporate information. Many recovery tools are also available to help end users rescue data from a corrupted hard disk. Assimilating into existing corporate identity controls, Endpoint Encryption has a variety of authentication methods, including Active Directory integration and resources for end users who have forgotten their credentials.

Key Features and Benefits

The following table explains Endpoint Encryption key features and benefits.

**TABLE 1-1. Endpoint Encryption Key Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>• Protection for the full disk, including the master boot record (MBR), operating system, and all system files</td>
</tr>
<tr>
<td></td>
<td>• Hardware-based and software-based encryption for mixed environments</td>
</tr>
<tr>
<td></td>
<td>• Comprehensive data protection of files, folders, and removable media</td>
</tr>
<tr>
<td>Feature</td>
<td>Benefits</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>• Flexible authentication methods, including both single and multi-factor&lt;br&gt;• Control password strength and regularity for password changes&lt;br&gt;• Policy updates before authentication and system boot&lt;br&gt;• Configurable actions on failed password attempt threshold</td>
</tr>
<tr>
<td>Device management</td>
<td>• Policies to protect data on endpoints and removable media&lt;br&gt;• Ability to remotely lock, reset, wipe, or kill a device</td>
</tr>
<tr>
<td>Central administration</td>
<td>• Flexibly use either PolicyServer MMC or Control Manager to manage PolicyServer&lt;br&gt;• Deploy Endpoint Encryption agents to endpoints already managed by OfficeScan&lt;br&gt;• Enforce security policies to individual users and policy groups from a single policy server&lt;br&gt;• Instantly protect end user data by sending lock or erase commands to lost or stolen Endpoint Encryption devices&lt;br&gt;• Automate policy enforcement with remediation of security events&lt;br&gt;• Update security policies in real-time, before authentication, to revoke user credentials before booting the operating system</td>
</tr>
<tr>
<td>Record keeping,</td>
<td>• Advanced real-time reporting and auditing to ensure security compliance&lt;br&gt;• Analyze usage statistics with scheduled reports and alert notifications</td>
</tr>
<tr>
<td>reports, and auditing</td>
<td></td>
</tr>
</tbody>
</table>

**What's New in Version 5.0**

Trend Micro Endpoint Encryption 5.0 includes many new features and enhancements.
### Table 1-2. What's New in Endpoint Encryption 5.0

<table>
<thead>
<tr>
<th><strong>New Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **New Communication Interface**    | Endpoint Encryption 5.0 introduces a new communication interface (Endpoint Encryption Service) that all Endpoint Encryption 5.0 agents and management consoles use to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. Endpoint Encryption Service has three key features:  
  - Access control: After user authentication, PolicyServer generates a token for that user in that session only.  
  - Policy control: Before user authentication, Endpoint Encryption Service restricts all PolicyServer MMC, Control Manager, and OfficeScan policy transactions until after user authentication.  
  - Automatic policy updates: After successfully registering with PolicyServer, Endpoint Encryption agents automatically obtain new policies without user authentication. |
| **Control Manager Integration**    | Endpoint Encryption 5.0 integrates Control Manager for PolicyServer management.  
For information about Control Manager, see *About Control Manager Integration on page 3-2.* |
| **OfficeScan Integration**         | Endpoint Encryption 5.0 provides support for OfficeScan deployments. Use the new Endpoint Encryption Deployment Tool plug-in to centrally deploy or uninstall Endpoint Encryption agents to any endpoint currently managed by OfficeScan. |
| **License Management**             | Endpoint Encryption 5.0 integrates with the Trend Micro licensing portal. As in previous product versions, you can try Endpoint Encryption free for 30 days. After the trial license expires, an Activation Code is required.  
For information about licensing, see *Maintenance Agreement on page 17-2.* |
**NEW FEATURE** | **DESCRIPTION**
---|---
Support for Apple FileVault™ and Microsoft BitLocker™ | Endpoint Encryption 5.0 advances Full Disk Encryption by integrating with encryption solutions built into the host operating system through two new Endpoint Encryption agents:
- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault
PolicyServer centrally manages both agents with policy controls to remotely wipe or kill the Endpoint Encryption device.

FileArmor Name Change and Move to Common Framework | Endpoint Encryption 5.0 renames the FileArmor agent to File Encryption to better match the Endpoint Encryption agent's new functionality. File Encryption has the benefits from FileArmor 3.1.3, including improved support for removable media.
File Encryption is also now better aligned with Full Disk Encryption for improved password and policy management.
### New Feature

<table>
<thead>
<tr>
<th><strong>New Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance, Log, and Report Enhancements</td>
<td>Endpoint Encryption 5.0 has several improvements to product maintenance, logs and reports.</td>
</tr>
<tr>
<td></td>
<td>• Mechanism to purge log database: It is now possible to purge the log database based on specific criteria. For more information, see Log Purge on page 16-7.</td>
</tr>
<tr>
<td></td>
<td>• Delete inactive Endpoint Encryption users and devices: To clean up the Enterprise devices and users, it is now possible to purge devices and users that are inactive for a specified time period. For more information, see Purge Inactive Devices on page 16-5.</td>
</tr>
<tr>
<td></td>
<td>• Enterprise report for inactive users: The new Enterprise report shows all Endpoint Encryption users who have not logged on Endpoint Encryption devices for a specified period of time. For more information, see the updated list of available standard reports at Standard Reports on page 16-17.</td>
</tr>
<tr>
<td></td>
<td>• Enterprise report for inactive devices: The new Enterprise report shows all Endpoint Encryption devices that have not been logged on to for a specified duration of time. For more information, see the updated list of available standard reports at Standard Reports on page 16-17.</td>
</tr>
<tr>
<td>Smart Card Enhancements</td>
<td>Endpoint Encryption 5.0 provides the following smart card enhancements:</td>
</tr>
<tr>
<td></td>
<td>• Improved Endpoint Encryption agent deployment in environments using smart cards</td>
</tr>
<tr>
<td></td>
<td>• Support for smart card password-sharing</td>
</tr>
</tbody>
</table>

### About Encryption

Encryption is the process of making data unreadable unless there is access to the encryption key. Perform encryption via software or hardware (or a combination of the two) to protect data locally on an endpoint hard drive, on removable media, or in
specific files and folders, and on data in transit across networks or the Internet. Endpoint encryption is the most important way to assure data security and to ensure that regulatory compliance mandates for data protection are met.

About FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 is a United States government device security standard that specifies the security requirements for encryption modules. The following table explains the four levels of FIPS 140-2 security:

TABLE 1-3. FIPS 140-2 Security Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Requires all encryption components to be production grade, and absent of obvious security holes.</td>
</tr>
<tr>
<td>2</td>
<td>Includes level 1 requirements and adds physical tamper-evidence and role-based authentication.</td>
</tr>
<tr>
<td>3</td>
<td>Includes level 2 requirements and adds physical tamper-resistance and identity-based authentication.</td>
</tr>
<tr>
<td>4</td>
<td>Includes level 3 requirements and adds additional physical security requirements.</td>
</tr>
</tbody>
</table>

Endpoint Encryption Components

Endpoint Encryption consists of one central management server (PolicyServer) that manages the policy and log databases, authentication, and all client-server activity. Deploy several unique Endpoint Encryption agents that each perform specific encryption tasks. All Endpoint Encryption agents communicate via an encrypted channel.

Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.
Endpoint Encryption integrates with OfficeScan. Use the Endpoint Encryption Deployment Tool plug-in to deploy the Endpoint Encryption agent software to any OfficeScan managed endpoint.

**Note**

For information about deployment scenarios, see *Deployment and Upgrade Overview* in the *Endpoint Encryption Installation and Migration Guide*.

The following illustration shows the Endpoint Encryption components and communication protocols.

*Figure 1-1. Endpoint Encryption Architecture*
The following table describes these components.

**TABLE 1-4. Endpoint Encryption Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Endpoint Encryption PolicyServer Services | PolicyServer consists of several services that centrally control policies, authentication, and reporting. PolicyServer consists of the following:  
  • Endpoint Encryption Service  
  • Legacy Web Service  
  • PolicyServer Windows Service  
  For information about PolicyServer, see *About PolicyServer on page 1-10.* |
| Endpoint Encryption PolicyServer SQL Database | The Microsoft™ SQL Server database stores all user, policy, and log information. Install the database on the same server as PolicyServer, or separately. Flexibly configure PolicyServer using Microsoft SQL Server or Microsoft SQL Express.  
  For information about database configuration options, see the *Endpoint Encryption Installation and Migration Guide.* |
| Endpoint Encryption PolicyServer MMC | PolicyServer MMC is the native interface option to remotely manage PolicyServer. |
| Trend Micro Control Manager | Trend Micro Control Manager is an option to remotely manage PolicyServer while also integrating with other managed Trend Micro products.  
  Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. |
## COMPONENT | DESCRIPTION
--- | ---
Endpoint Encryption 5.0 agents | All Endpoint Encryption 5.0 agents communicate with the PolicyServer Endpoint Encryption Service using a RESTful web API.
For more information about Endpoint Encryption agents, see:
- *About Full Disk Encryption on page 14-2*
- *About File Encryption on page 13-2*
For information about Endpoint Encryption agent communications, see *About PolicyServer on page 1-10*.

**Note**
Configure port settings during Endpoint Encryption agent installation. Full Disk Encryption can use Recovery Console to change the assigned port number.

Other Endpoint Encryption agents | All legacy Endpoint Encryption agents (3.1.3 and older) communicate to the Legacy Web Service on PolicyServer. For details about agent communications, see *About PolicyServer on page 1-10*.

Active Directory | PolicyServer synchronizes user account information by communicating with Active Directory using LDAP. Account information is cached in the Microsoft SQL database.

**Note**
Active Directory is optional.

### About PolicyServer

Trend Micro PolicyServer manages encryption keys and synchronizes policies across all endpoints in the organization. PolicyServer also enforces secure authentication and provides real-time auditing and reporting tools to ensure regulatory compliance. You can flexibly manage PolicyServer with PolicyServer MMC or with Trend Micro Control
Manager. Other data management features include user-based self-help options and device actions to remotely reset or “kill” a lost or stolen device.

The following table describes the PolicyServer components that you can deploy on one server or multiple servers, depending on environmental needs.

**TABLE 1-5. PolicyServer Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured when installing PolicyServer. One PolicyServer database may have one Enterprise configuration.</td>
</tr>
<tr>
<td>Database</td>
<td>The PolicyServer Microsoft SQL database securely stores all user, device, and log data. The database is either configured on a dedicated server or added to an existing SQL cluster. The log and other databases can reside separately.</td>
</tr>
<tr>
<td>PolicyServer Windows Service</td>
<td>PolicyServer Windows Service manages all communication transactions between the host operating system, Endpoint Encryption Service, Legacy Web Service, Client Web Proxy, and SQL databases.</td>
</tr>
<tr>
<td>Endpoint Encryption Service</td>
<td>All Endpoint Encryption 5.0 agents use Endpoint Encryption Service to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Until the Endpoint Encryption user authenticates, the service denies all policy transactions. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall. For information about deployment scenarios, see the <em>Endpoint Encryption Installation and Migration Guide</em>.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Legacy Web Service</td>
<td>All Endpoint Encryption 3.1.3 and older agents use Simple Object Access Protocol (SOAP) to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall. For information about deployment scenarios, see the <em>Endpoint Encryption Installation and Migration Guide</em>.</td>
</tr>
</tbody>
</table>

**Management Consoles**

Depending on endpoint security and existing infrastructure needs, you can manage Endpoint Encryption using only one management console or a combination of several management consoles. The following table describes the management consoles available to manage Endpoint Encryption.
### Table 1-6. Endpoint Encryption Management Consoles

<table>
<thead>
<tr>
<th>Management Console</th>
<th>Description</th>
</tr>
</thead>
</table>
| PolicyServer MMC   | The PolicyServer Microsoft Management Console plug-in (PolicyServer MMC) is the native management console for Endpoint Encryption policy, user, and device administration. Use PolicyServer MMC to centrally manage:  
  - All Endpoint Encryption users, devices, and groups  
  - All policies including encryption, password complexity and authentication  
  - Remote device actions, including killing a device, erasing data, or delaying authentication  
  - Event logs about authentication events, management events, device encryption status, and security violations  
  - Remote Help password reset process  
  - Auditing and reporting options |
**Management Console** | **Description** |
--- | --- |
Control Manager | Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Create multilayer security by integrating Endpoint Encryption with Control Manager as a managed Trend Micro product. Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting. |
OfficeScan | OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents. Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to centrally deploy or uninstall Endpoint Encryption agents to any endpoint currently managed by OfficeScan. |

**Endpoint Encryption Agents**

The following table describes the Endpoint Encryption agents available for a variety of environments.
<table>
<thead>
<tr>
<th>Agent</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Encryption</td>
<td>The Endpoint Encryption agent for file and folder encryption on local drives and removable media. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. For more information, see <em>About File Encryption on page 13-2</em>.</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Use Full Disk Encryption to secure data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated. For more information, see <em>About Full Disk Encryption on page 14-2</em>.</td>
</tr>
<tr>
<td>Encryption Management for Microsoft BitLocker</td>
<td>The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint. Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. For more information, see <em>About Full Disk Encryption on page 14-2</em>.</td>
</tr>
<tr>
<td>Encryption Management for Apple FileVault</td>
<td>The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. For more information, see <em>About Full Disk Encryption on page 14-2</em>.</td>
</tr>
</tbody>
</table>
Note

Endpoint Encryption 5.0 does not have KeyArmor devices. However, legacy KeyArmor devices are supported.
Chapter 2

Devices and Users Overview

This chapter explains how Endpoint Encryption protects user identity and endpoint access. Correctly configuring Endpoint Encryption users, policy groups, and devices ensures that data remains encrypted from unauthorized users, thus preventing data loss risk from accidental information release or deliberate sabotage.

Topics include:

• Endpoint Encryption Devices on page 2-2
• Endpoint Encryption Users on page 2-4
• Authentication Methods on page 2-6
Endpoint Encryption Devices

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

You can set policy rules that automatically trigger after too many failed authentication attempts or when the Endpoint Encryption agent has outdated policies. The following policy rules are available:

- Time delay
- Remote authentication required
- Erase device

PolicyServer can instantly act upon a lost or stolen endpoint by initiating a remote action upon the associated Endpoint Encryption device. The following remote actions are available:

- Software token
- Recovery key
- Kill device
- Lock device
- Soft reset

Endpoint Encryption Device Policy Rules

The following table explains the security policy rules for lost or stolen Endpoint Encryption devices. Depending on the policy settings, too many consecutive unsuccessful authentication attempts to the Endpoint Encryption devices delays the next authentication attempt, locks the Endpoint Encryption device, or erases all data controlled by the associated Endpoint Encryption agent.
TABLE 2-1. Device Security Options

<table>
<thead>
<tr>
<th>SECURITY OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time delay</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer temporarily locks the Endpoint Encryption device and notifies the Endpoint Encryption user that the device is locked. The ability to authenticate or reset the password is disabled during the time delay. The duration of the time delay is determined by policy. Once the time delay has expired, the user is permitted to authenticate.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The Endpoint Encryption user may use Self Help or Remote Help authentication to avoid waiting for the time delay period to expire.</td>
</tr>
<tr>
<td>Remote authentication required</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer locks the Endpoint Encryption device until the Endpoint Encryption user contacts Technical Support for Remote Help authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For more information, see Remote Help on page 2-11.</td>
</tr>
<tr>
<td>Erase the device</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer erases all data controlled by the associated Endpoint Encryption agent. For example, erasing a Full Disk Encryption device deletes all data from the endpoint, while erasing a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong></td>
</tr>
<tr>
<td></td>
<td>The Endpoint Encryption user cannot recover the erased data.</td>
</tr>
</tbody>
</table>

Endpoint Encryption Device Remote Actions

The following table explains the remote actions that PolicyServer can send to the Endpoint Encryption device.
### Table 2-2. Endpoint Encryption Device Security

<table>
<thead>
<tr>
<th>Device Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Token</td>
<td>Generating a “software token” creates a unique string that you can use to unlock Endpoint Encryption devices and to remotely help Endpoint Encryption users reset forgotten passwords.</td>
</tr>
<tr>
<td>Recovery Key</td>
<td>Generating a “recovery key” allows the user to decrypt a hard disk when the user has forgotten the original password or key. The recovery key is only available to Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker agents because they do not use the other recovery methods available in Full Disk Encryption.</td>
</tr>
<tr>
<td>Kill device</td>
<td>Initiating a “kill” command deletes all Endpoint Encryption device data. The deleted data is different depending on the scope of data that the associated Endpoint Encryption agent manages. For example, initiating a “kill” command to a Full Disk Encryption device deletes all data from the endpoint, while initiating a “kill” command to a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent. The “kill” command is issued when the Endpoint Encryption agent communicates with PolicyServer.</td>
</tr>
<tr>
<td>Lock device</td>
<td>Initiating a “lock” command to the Endpoint Encryption device prevents Endpoint Encryption user access until after performing a successful Remote Help authentication. Locking a device reboots the endpoint and forces it into a state that requires Remote Help. The lock command is issued when the Endpoint Encryption agent communicates with PolicyServer.</td>
</tr>
<tr>
<td>Soft reset</td>
<td>Initiating a “soft reset” command reboots the endpoint. The command issues the next time that the agent communicates with PolicyServer.</td>
</tr>
</tbody>
</table>

### Endpoint Encryption Users

Endpoint Encryption users are any user account manually added to PolicyServer or synchronized with Active Directory.

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Control Manager
or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

### Endpoint Encryption User Roles

The following table explains the Endpoint Encryption user account types intended for different roles within the Enterprise or policy group. Each role determines the permissions granted when the user accesses Endpoint Encryption management consoles and devices.

**TABLE 2-3. Endpoint Encryption Account Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Administrator</td>
<td>Intended for administrators who control the Enterprise and require administrative rights to all groups, users, devices, and policies regardless of where they reside.</td>
</tr>
<tr>
<td>Group or Policy Administrator*</td>
<td>Intended for administrators who control any assigned group or policy.</td>
</tr>
<tr>
<td>Note</td>
<td>Privileges do not apply to parent groups, groups at the same level in the hierarchy or their subgroups.</td>
</tr>
<tr>
<td>Enterprise Authenticator</td>
<td>Intended for Help Desk personnel who provide remote assistance when users forget their Endpoint Encryption password or have a technical problem. Enterprise Authenticators have configurable privileges for the Enterprise.</td>
</tr>
<tr>
<td>Group or Policy Authenticator*</td>
<td>Intended for Help Desk personnel with the same privileges as the Enterprise Authenticator except for being limited to the assigned group or policy only.</td>
</tr>
<tr>
<td>User</td>
<td>Intended for basic end users with no special privileges. The user role cannot log on to Endpoint Encryption management consoles.</td>
</tr>
</tbody>
</table>
Note

*Due to differences in policy architecture, Control Manager merges the policy and group structure of PolicyServer MMC. The following roles are the same between PolicyServer MMC and Control Manager:

- Group Administrator (PolicyServer MMC) and Policy Administrator (Control Manager)
- Group Authenticator (PolicyServer MMC) and Policy Authenticator (Control Manager)

Authentication Methods

Endpoint Encryption administrators and users have several authentication methods to log on to Endpoint Encryption devices. The methods available are determined by the PolicyServer policy configuration.

**Table 2-4. Supported Authentication Methods**

<table>
<thead>
<tr>
<th>AUTHENTICATION METHOD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ColorCode™</td>
<td>A unique sequence of colors.</td>
</tr>
<tr>
<td>Domain authentication</td>
<td>Active Directory LDAP synchronization for single sign-on (SSO).</td>
</tr>
<tr>
<td>Fixed password</td>
<td>A string of characters, numbers, and symbols.</td>
</tr>
<tr>
<td>PIN</td>
<td>A standard Personal Identification Number (PIN).</td>
</tr>
<tr>
<td>Remote Help</td>
<td>Interactive authentication for users who forget their credentials or devices that have not synchronized policies within a predetermined amount of time.</td>
</tr>
<tr>
<td>Self Help</td>
<td>Question and answer combinations that allow users to reset a forgotten password without contacting Technical Support.</td>
</tr>
<tr>
<td>Smart card</td>
<td>A physical card used in conjunction with a PIN or fixed password.</td>
</tr>
</tbody>
</table>
Important Note About PolicyServer MMC Requirement

You must use PolicyServer MMC to configure the authentication methods available to Endpoint Encryption users. It is not possible to use Control Manager to configure the allowed authentication methods. However, you can configure Control Manager for domain authentication.

In PolicyServer MMC, configure policies for each Endpoint Encryption agent.

• For Full Disk Encryption, see Password Policies on page 9-25.
• For File Encryption, see Login Policies on page 9-28.

Note
Remote Help authentication is triggered by Endpoint Encryption device policy rules. Remote Help policy rules are configurable in both PolicyServer MMC and Control Manager. For more information, see Remote Help Policy Rules on page 2-11.

For information about configuring domain authentication, see Domain Authentication Policy Rules on page 2-10.

Authentication Restrictions

The following table explains the authentication options available in PolicyServer MMC and the Endpoint Encryption agents.

**Table 2-5. Authentication Restrictions**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Authentication Option</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fixed Password</td>
</tr>
<tr>
<td>PolicyServer MMC</td>
<td>●</td>
</tr>
<tr>
<td>Control Manager</td>
<td>●</td>
</tr>
<tr>
<td>OfficeScan</td>
<td>●</td>
</tr>
<tr>
<td>Agent</td>
<td>Authentication Option</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>Fixed Password</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>●</td>
</tr>
<tr>
<td>File Encryption</td>
<td>●</td>
</tr>
<tr>
<td>KeyArmor</td>
<td>●</td>
</tr>
</tbody>
</table>

**Note**

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**ColorCode**

ColorCode™ is a unique authentication method designed for quick access and easy memorization. Rather than alphanumeric characters or symbols for the password,
ColorCode authentication consists of a user-created color sequence (example: red, red, blue, yellow, blue, green).

**Figure 2-1. ColorCode Authentication Screen**

**Domain Authentication**

Endpoint Encryption integrates with Active Directory using LDAP configured in PolicyServer. Endpoint Encryption domain authentication allows Endpoint Encryption users to use single sign-on (SSO) between the operating system and the Endpoint Encryption agent. For example, Endpoint Encryption users with domain authentication must only provide their credentials once to authenticate to the Full Disk Encryption preboot, log on to Windows, and access the files protected by File Encryption.

For seamless Active Directory integration, make sure that the following requirements are met:

- All Endpoint Encryption devices are in the same domain as PolicyServer.
- The user name configured in Active Directory exactly matches the user name configured in PolicyServer (including case).
• The user name is located within a PolicyServer group and the Domain Authentication policy is enabled.

• The host name and domain name are configured correctly based on the LDAP or Active Directory server settings.

---

**Note**

For information about configuring LDAP and Active Directory settings, see the *Endpoint Encryption Installation and Migration Guide* available at:


---

**Domain Authentication Policy Rules**

Enable domain authentication using one of the following methods:

• In Control Manager, edit or modify a policy's **Users** rules.

  For more information, see *Configuring Endpoint Encryption Users Rules on page 3-14*.

• In PolicyServer MMC, go to **[Group Name]** > **Policies** > **Common** > **Authentication** > **Network Login** > **Domain Authentication**.

---

**Note**

For information about configuring LDAP and Active Directory settings, see the *Endpoint Encryption Installation and Migration Guide* available at:


---

**Fixed Password**

Fixed password authentication is the most common authentication method. The fixed password is created by the user and can be almost any string of numbers, characters, or symbols. You can place restrictions on fixed passwords to ensure that they are not easily compromised.
PIN

A Personal Identification Number (PIN) is a common identification method requiring a unique sequence of numbers. The PIN is created by the user and can be almost anything. Similar to fixed passwords, you may place restrictions on the PIN combination.

Remote Help

Remote Help allows Group or Enterprise Authenticators to assist Endpoint Encryption users who are locked out and cannot log on to Endpoint Encryption devices after too many unsuccessful log on attempts, or when the period between the last PolicyServer synchronization has been too long.

Remote Help Policy Rules

The following table describes the locations of the account lockout and device lock policies that affect Remote Help authentication. Use it to understand which policies are appropriate to set.

**Table 2-6. Remote Help Policy Locations**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>PolicyServer MMC Menu Path</th>
<th>Control Manager MMC Menu Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Action</td>
<td>Login &gt; Account Lockout Action</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Account Lockout Action</td>
<td>The action taken when the length of time in “Account Lockout Actions” include: erase, remote authentication.</td>
</tr>
<tr>
<td>Account Lockout Period</td>
<td>Login &gt; Account Lockout Period</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Lock account after [ ] days</td>
<td>The number of days that a device can not communicate with PolicyServer before “Account Lockout Action” is called.</td>
</tr>
<tr>
<td>POLICY NAME</td>
<td>POLICY SERVER MMC MENU PATH</td>
<td>CONTROL MANAGER MMC MENU PATH</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Locked Action</td>
<td>For each agent: Login &gt; Device Locked Action</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Device locked action</td>
<td>The action taken when the “Failed Attempts Allowed” policy value has been exceeded. Actions include: time delay, erase, remote authentication.</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>For each agent: Login &gt; Failed Login Attempts Allowed</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Failed logon attempts allowed</td>
<td>The number of failed login attempts allowed before executing the action defined in “Device Locked”.</td>
</tr>
</tbody>
</table>

**Self Help**

Self Help authentication allows Endpoint Encryption users who have forgotten the credentials to answer security questions and log on to Endpoint Encryption devices without getting Technical Support assistance. Self Help is not available to Enterprise or Group Administrator and Authenticator accounts. Self Help requires the Endpoint Encryption user to respond with answers to predefined personal challenge questions. Self Help can replace fixed password or other authentication methods.

---

**Note**

Self Help is only configurable with PolicyServer MMC.

Make sure to allow Self Help authentication. For more information, see [Authentication Policies](#) on page 9-30.

---

**WARNING!**

Self Help can have a maximum of six questions. Do not create more than six questions or users cannot log on using Self Help authentication.
### Smart Card

Smart card authentication requires both a PIN and a physical token to confirm the user identity. To use smart card authentication, make sure that the following requirements are met:

- The smart card reader is connected to the endpoint and the smart card is inserted into the smart card reader.
- ActivClient 6.1 with all service packs and updates are installed.
- Specify the smart card PIN in the password field.

---

**WARNING!**

Failure to provide a correct password sends a password error and may result in locking the smart card.

---

**Note**

Smart card authentication is only configurable with PolicyServer MMC.

Enable smart card authentication for each Endpoint Encryption agent:

- For File Encryption, go to **Login > Password > Physical Token Required**.
- For Full Disk Encryption, go to **Full Disk Encryption > Login > Token Authentication**

### Smart Card Registration

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

Use one of the following methods to register a smart card:

- To use the Full Disk Encryption preboot, see *Registering a Smart Card in Full Disk Encryption Preboot on page 11-25*. 
To use PolicyServer MMC, see Configuring Smart Card Authentication in PolicyServer MMC on page 11-24.
Part II

Administration with Trend Micro Control Manager
Chapter 3

Getting Started with Control Manager

This chapter explains how to get started using Trend Micro Control Manager to manage PolicyServer.

Topics include:

•  About Control Manager Integration on page 3-2
•  Control Manager Architecture on page 3-3
•  Configuring Control Manager Summary of Operations on page 3-6
•  Adding PolicyServer as a Managed Product to Control Manager on page 3-7
•  Configuring Directory Management for PolicyServer on page 3-9
•  Creating a Policy on page 3-10
About Control Manager Integration

Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up to date. Example update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

The following illustration explains how to deploy Endpoint Encryption for the first time using Control Manager to manage PolicyServer. In a Control Manager deployment, administrators use Control Manager for all Endpoint Encryption policy, user, and device controls, and only use PolicyServer MMC for advanced Enterprise maintenance.
In environments that use Control Manager, changes to PolicyServer policies are always controlled by Control Manager. Any changes made using PolicyServer MMC are overwritten the next time that Control Manager synchronizes policies to the PolicyServer database.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a
corporate virus/malware and content security policy. The following table provides a list of components Control Manager uses.

**Table 3-1. Control Manager Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Control Manager server | Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features:  
• An SQL database that stores managed product configurations and logs  
  Control Manager uses the Microsoft SQL Server database *(db_ControlManager.mdf)* to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.  
• A web server that hosts the Control Manager web console  
• A mail server that delivers event notifications through email messages  
  Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure Event Center to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification.  
• A report server, present only in the Advanced Edition, that generates antivirus and content security product reports  
  A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network. |
### Trend Micro Management Communication Protocol

MCP handles the Control Manager server interaction with managed products that support the next generation agent.

MCP is the new backbone for the Control Manager system.

MCP agents install with managed products and use one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.

### Trend Micro Management Infrastructure

Handles the Control Manager server interaction with older managed products.

The Communicator, or the Message Routing Framework, is the communication backbone of the older Control Manager system. It is a component of the Trend Micro Management Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. They interact with Control Manager 2.x agents to communicate with older managed products.

### Control Manager 2.x Agents

Receives commands from the Control Manager server and sends status information and logs to the Control Manager server.

The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Therefore, install agents on the same computer as managed products.

### Web-based management console

Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™

The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget Framework</td>
<td>Allows an administrator to create a customized dashboard to monitor the Control Manager network.</td>
</tr>
</tbody>
</table>

### Configuring Control Manager Summary of Operations

The following procedure provides an overview to configure Control Manager for Endpoint Encryption management.

**Note**

For information about individual policy configurations, see *Policies in Control Manager on page 5-1.*

**Procedure**

1. Install and configure PolicyServer.
   
   See the *Endpoint Encryption Installation and Migration Guide.*

2. Connect PolicyServer to Control Manager.
   
   a. *Adding PolicyServer as a Managed Product to Control Manager on page 3-7*
   
   b. *Configuring Directory Management for PolicyServer on page 3-9*

3. Add policy targets.
   
   See *Creating a Policy on page 3-10.*

4. Verify the policy configuration on PolicyServer MMC.
Adding PolicyServer as a Managed Product to Control Manager

Endpoint Encryption allows administrators to use Trend Micro Control Manager to control PolicyServer and manage Endpoint Encryption agent policies or use Trend Micro OfficeScan to deploy Endpoint Encryption agent software on managed endpoints.

To use Control Manager to manage PolicyServer, you must add PolicyServer as a managed product.

Make sure to complete the following tasks before proceeding:

1. Install and configure Control Manager.
   See the supporting documentation at:

2. Install and configure PolicyServer.
   See the Endpoint Encryption Installation and Migration Guide.

**Important**

Endpoint Encryption supports only one configured PolicyServer instance in Control Manager at a time. It is not possible to add multiple PolicyServer configurations. To configure a different PolicyServer, first remove the previously configured PolicyServer.

**Procedure**

1. Review all system requirements for compatible product versions.
   See the Endpoint Encryption Installation and Migration Guide.

2. Log on to Control Manager.

   The Managed Servers screen appears.

4. In the Server Type drop-down list, select Endpoint Encryption.
5. Click **Add**.

The **Add Server** screen appears.

![Add Server Screen](image)

6. Specify **Server Information** options.

   - **Server**: Specify the PolicyServer host name and the port number. Use the following format:

     
     http(s)://<server_name>:port_number

   - **Note**: Control Manager communicates with PolicyServer Endpoint Encryption Service. The default port number is 8080.

   - **Display name**: Specify how PolicyServer shows in the **Managed Servers** screen

7. Under **Authentication**, specify the user name and password of the Endpoint Encryption Enterprise Administrator account.

8. Under **Connection**, select **Use a proxy server for the connection** if PolicyServer requires a proxy connection.
9. Click **Save**.

---

**Note**

Synchronization between Control Manager and PolicyServer may require several minutes to complete.

---

PolicyServer is added as a new managed product to Control Manager.

---

### Configuring Directory Management for PolicyServer

The following procedure explains how to configure Directory Management for the new PolicyServer data source. Directory Management is represented in the directory tree when creating policy targets. For details about the **Directory Management** screen, see *Understanding the Product Directory on page A-15*.

Make sure to add PolicyServer to Control Manager as a managed server before starting this procedure. For more information, see *Adding PolicyServer as a Managed Product to Control Manager on page 3-7*.

---

**Procedure**

1. Go to **Policies > Policy Resources > Managed Servers**.

   The **Managed Servers** screen appears.

2. Click **Directory Management**.
The **Directory Management** screen appears.

3. Select the server and then click **Add Folder**.

   The **Add Directory** screen appears.

4. Specify a directory name and then click **Save**.

5. Click **OK** to confirm.

   The new folder is created.

6. Drag the previously added PolicyServer data source into the new folder.

7. Click **OK** to confirm.

8. Click **< Back** to return to the **Policy Management** screen.

---

**Creating a Policy**

The following procedure explain how to configure a Control Manager policy that affects Endpoint Encryption users and devices.

---

**Important**

To add a user account to the policy, make sure that the user account already exists.
Note

For information about available policy settings, see *Endpoint Encryption Policy Settings on page 5-12.*

For information about adding new Endpoint Encryption users, see *Adding Users to Endpoint Encryption on page 6-4.*

For information about configuring Active Directory, see the *Endpoint Encryption Installation and Migration Guide.*

For information about policy mapping between Control Manager and PolicyServer MMC, see *Policy Mapping Between Management Consoles on page D-1.*

Procedure

1. Go to **Policies > Policy Management.**
2. From the **Product** drop-down list, select **Endpoint Encryption.**
3. Click **Create.**

The Create Policy screen appears.

4. Specify a policy name.
5. Select one of the following policy target options:

   - **None (Draft Only):** Create a policy with no targets (endpoints)
   - **Filter by Criteria:** Endpoint Encryption does not support filtering by criteria
   - **Specify Target(s):** Specify existing endpoints.

   **Note**
   For more information about policy targets, see *Specifying Policy Targets on page 3-12*


   - Configure **User** policies.
     See *Configuring Endpoint Encryption Users Rules on page 3-14*.
   - Configure **Full Disk Encryption** policies.
     See *Configuring Full Disk Encryption Rules on page 3-15*.
   - Configure **File Encryption** policies.
     See *Configuring File Encryption Rules on page 3-17*.
   - Configure **Common** policies.
     See *Configuring Common Policy Rules on page 3-19*.

7. Click **Save**.

---

**Specifying Policy Targets**

Use the **Specify Target(s)** screen to assign Endpoint Encryption devices to the policy.

**Note**

The **Specify Target(s)** screen is available when creating a new policy. For information about creating a policy, see *Creating a Policy on page 3-10*. 

---
**Figure 3-1. Specifying Policy Targets**

**Procedure**

1. From the **Specify Target(s)** screen, click the **Browse** tab.

2. From the left pane, expand the tree to select the managed folder.
   
   Example: **CM-PI-2K8 > Local Folder > TMEE > TMEE > QA2**

3. Select any appropriate Endpoint Encryption devices, or select the top check box to select all Endpoint Encryption devices listed on the current page.

4. Click **Add Selected Targets**.

**Note**

To immediately select all devices in the managed folder, click **Add All from Selected Folder**.

“View Action List” and “View Results” update based on the selection.
5. Click OK.

Configuring Endpoint Encryption Users Rules

The following procedure explains the configurable options for policy rules affecting authentication and Endpoint Encryption user accounts.

Procedure

1. Create a new Endpoint Encryption policy.

   See Creating a Policy on page 3-10.

2. Click Users.

   The Users policy rules settings appear.

3. Under Domain User Settings, select Enable domain authentication to specify whether users require domain authentication.

![Figure 3-2. Endpoint Encryption Users Policy Rules](image)
**Important**

Active Directory (AD) synchronization requires PolicyServer to have three enabled components:

a. Configure the AD domain.

b. Configure the policy group to point to the proper Organizational Unit (OU).

c. Configure the policy group with appropriate credentials to access the AD domain that matches the policy group's “Distinguished Name”.

To configure domain authentication, see PolicyServer Active Directory Synchronization in the Endpoint Encryption Installation and Migration Guide.


   • Select **All Endpoint Encryption users** to allow all users, domain and local accounts, to authenticate Endpoint Encryption devices.

   • Select **Select specific users** to specify which already added Endpoint Encryption users can authenticate to managed endpoints.

**Note**

Policy rules only affect existing user accounts. Before configuring policies, add new users with the Endpoint Encryption Users Widget. For more information, see *Adding Users to Endpoint Encryption on page 6-4*.

---

**Configuring Full Disk Encryption Rules**

The following procedure explains the configurable options for policy rules affecting Full Disk Encryption devices.

**Note**

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.
Procedure

1. Create a new Endpoint Encryption policy.
   See Creating a Policy on page 3-10.

2. Click Full Disk Encryption.
   The Full Disk Encryption policy rules settings appear.

3. Under Encryption, select Encrypt device to start full disk encryption when the Endpoint Encryption agent synchronizes policies with PolicyServer.

   **WARNING!**
   Do not deploy encryption to Full Disk Encryption agents without first preparing the endpoint's hard drive.
   For information about preparing the hard drive, see Full Disk Encryption Deployment Outline in the Endpoint Encryption Installation Guide.

4. Under Agent Settings, select the following options:
• Select **Bypass Full Disk Encryption Preboot** to allow the user to authenticate directly into Windows without protection from preboot authentication.

• Select **Users are allowed to access system recovery utilities on the device** to allow the user to access the Recovery Console.

For information about configurable options and available tools in Full Disk Encryption, see *Full Disk Encryption Recovery Console on page 14-20.*

5. Under **Notifications**, configure the following options:

• Select **If found, display the following message on the device** to show a message when the **If Found** policy is active.

• Select **Display Technical Support contact information** to show a message after the user logs on to the Full Disk Encryption agent.

• Select **Show a legal notice** to show the specific legal message at start up or only after installing the Full Disk Encryption agent.

---

**Configuring File Encryption Rules**

The following procedure explains the configurable options for policy rules affecting File Encryption devices.

---

**Procedure**

1. Create a new Endpoint Encryption policy.

   See *Creating a Policy on page 3-10.*

2. Click File Encryption.
The **File Encryption** policy rules settings appear.

**Figure 3-4. File Encryption Policy Rules**

3. Under **Folder to Encrypt**, specify folders that are automatically created and encrypted on the endpoint when the File Encryption agent synchronized policies.

4. Under **Encryption Key**, select the encryption for the File Encryption encrypted folder.
   - **User key**: Use a unique key for each Endpoint Encryption user. Only the Endpoint Encryption user can decrypt files that he or she encrypted.
• **Policy key**: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can decrypt files.

• **Enterprise key**: Any Endpoint Encryption user or device in the Enterprise can decrypt the files.

---

**Note**

Selecting **Policy key** or **Enterprise key** controls the sharing for the File Encryption shared key. For more information, see *File Encryption Shared Key Encryption on page 13-15*.

---

5. Under **Storage Devices**, configure the following options:

- Select **Disable optical drives** to control whether removable media is accessible from the endpoint.

- Select **Disable USB drives** to control when the USB ports are disabled. Options are:
  - **Always**
  - **Logged out**
  - **Never**

- Select **Encrypt all files and folders on USB devices** to automatically encrypt all the files and folders on removable drives when plugged into the endpoint.

- Select **Specify the file path to encrypt on USB devices** to add or remove encrypted folders to USB drives. If a folder does not exist, it is created. If no drive letter is specified, all USB devices are affected.

6. Under **Notifications**, select **Show a legal notice** to show the specific legal message at start up or only after installing the File Encryption agent.

---

**Configuring Common Policy Rules**

This section explains the configurable options for policy rules affecting all Endpoint Encryption devices.
Procedure

1. Create a new Endpoint Encryption policy.
   See Creating a Policy on page 3-10.

2. Click Common.

   ![Common Policy Rules](image)

   **Figure 3-5. Common Policy Rules**

3. Under Allow User to Uninstall, select **Allow User (non-administrator) accounts to uninstall agent software** to allow any Endpoint Encryption user to uninstall the agent.
By default, only Enterprise Administrator accounts can uninstall Endpoint Encryption agents.

4. Under **Lockout and Lock Device Actions**, configure the following options:
   
   - Select **Lock account after <number> days** to specify the number of days that the Endpoint Encryption device locks if it does not synchronize policies.
   
   - Use **Account lockout action** to specify whether the remote authentication or erase action occurs at lockout.

   **Note**
   For information about lock options, see *Account Lockout and Device Lock Actions on page 3-22*

   - Select **Failed log on attempts allowed** to specify how many times that a user can attempt to authenticate before the Endpoint Encryption device locks.
   
   - For Full Disk Encryption or File Encryption devices, separately configure the following:
     
     - Use **Device locked action** to specify whether the “Remote Authentication” or the “Erase” action occurs at lockout.

   **Note**
   For information about lock options, see *Account Lockout and Device Lock Actions on page 3-22*

   - Use **Number of minutes to lock device** to specify the duration that time delay locks the Endpoint Encryption device from authentication.

5. Under **Password**, configure the following options:
   
   - Select **Users must change password after <number> days** to control when a user is prompted to update password.
• Select **Users cannot reuse the previous <number> passwords** to specify how many previous passwords the user may reuse.

• Select **Number of consecutive characters allowed in a password** to specify how many repeated characters a user may specify in the password.

• Select **Minimum length allowed for passwords** to specify how many characters the user is required to use in the password.

6. Under **Password Requirements**, specify the password character limitations.

• **Letters**
• **Lowercase characters**
• **Uppercase characters**
• **Numbers**
• **Symbols**

---

**Important**

The sum total of letters, numbers, and symbols cannot exceed 255 characters.

---

**Account Lockout and Device Lock Actions**

Some policies have settings to lock out a user account or to lock a device based on certain criteria. Account lockout and device lock actions affect the Endpoint Encryption device whether or not the agent synchronizes policies with PolicyServer. For example, if the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time, the Endpoint Encryption agent automatically locks the Endpoint Encryption device. Use the tables below to understand the actions available for the account lockout and device lock actions.
Table 3-2. Account Lockout Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote authentication</td>
<td>Users cannot log on to the Endpoint Encryption device until after Technical Support provides remote authentication assistance.</td>
</tr>
<tr>
<td>Erase</td>
<td>All data is erased the next time that the agent synchronizes policies.</td>
</tr>
</tbody>
</table>

Note

Account lockout actions take effect when the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time (set by policy).

Table 3-3. Device Lock Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase</td>
<td>All data is erased the next time that the Endpoint Encryption agent synchronizes policies.</td>
</tr>
<tr>
<td>Remote authentication</td>
<td>Users cannot log on to Endpoint Encryption devices until after Technical Support provides remote authentication assistance.</td>
</tr>
<tr>
<td>Time delay</td>
<td>Users cannot log on to Endpoint Encryption devices for a specified time duration.</td>
</tr>
</tbody>
</table>

Note

Device lock actions take effect when the Endpoint Encryption user has too many unsuccessful logon attempts to that Endpoint Encryption device (set by policy).

Remote Help Policy Rules

The following table describes the locations of the account lockout and device lock policies that affect Remote Help authentication. Use it to understand which policies are appropriate to set.
### Table 3-4. Remote Help Policy Locations

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Policy Server MMC Menu Path</th>
<th>Control Manager MMC Menu Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Action</td>
<td>Login &gt; Account Lockout Action</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Account Lockout Action</td>
<td>The action taken when the length of time in “Account Lockout Actions” include: erase, remote authentication.</td>
</tr>
<tr>
<td>Account Lockout Period</td>
<td>Login &gt; Account Lockout Period</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Lock account after [ ] days</td>
<td>The number of days that a device can not communicate with PolicyServer before “Account Lockout Action” is called.</td>
</tr>
<tr>
<td>Device Locked Action</td>
<td>For each agent: Login &gt; Device Locked Action</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Device locked action</td>
<td>The action taken when the “Failed Attempts Allowed” policy value has been exceeded. Actions include: time delay, erase, remote authentication.</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>For each agent: Login &gt; Failed Login Attempts Allowed</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Failed logon attempts allowed</td>
<td>The number of failed login attempts allowed before executing the action defined in “Device Locked”.</td>
</tr>
</tbody>
</table>
Chapter 4

Dashboard, Widgets, and Reports

This chapter explains how to use the Control Manager dashboard, manage widgets, and run reports.

Topics include:

• Using the Dashboard on page 4-2
• Understanding Tabs on page 4-2
• Understanding Widgets on page 4-4
• Using Endpoint Encryption Widgets on page 4-8
Using the Dashboard

The Control Manager dashboard provides at-a-glance information for the Control Manager network. The dashboard is comprised of two components:

- **Tabs**: Allow administrators to create a screen that contains one or more widgets
- **Widgets**: Provide specific information about various security-related events

User Accounts and the Dashboard

Each user account displays its own dashboard. When a user logs on to Control Manager for the first time, the default tabs and the widgets contained within the tabs appear on the dashboard.

Each user account can customize the dashboard, tabs, and widgets for the account’s specific needs. Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Understanding Tabs

To customize the Control Manager Dashboard, add additional tabs, name the new tabs as needed, and add the appropriate widgets. You can modify or delete added tabs.

Default Tabs

The dashboard provides the following tabs:

- Summary
- DLP Incident Investigation
- Data Loss Prevention
- Compliance
Dashboard, Widgets, and Reports

- Threat Detection
- Smart Protection Network

**Note**
Deleting the default tabs permanently removes the tabs from viewing for the user account that removed the tabs. There is no way to recover a deleted tab. Deleting a default tab has no impact on the dashboard for other user accounts.

### Adding a New Tab

**Procedure**

1. Go to the **Dashboard**.
2. Click the + to the right of the last named tab. The **New Tab** screen appears.
3. Specify a name for the **Title** of the new tab.
4. Select the radio button for the appropriate layout style.
5. Select **Auto-fit On** to make the height all widgets on the tab consistent.
6. Click **Save**.

The new tab is added to the right of existing tabs.

### Modifying Tab Settings

**Procedure**

1. Go to the **Dashboard** and then open the appropriate tab.
2. Click **Tab Settings** at the upper-right corner of the tab.
3. Make the needed changes to:
   - Title
   - Layout
   - Auto-fit
4. Click Save.

---

**Deleting a Tab**

**Note**
Deleting the default tabs permanently removes the tabs from viewing for the user account that removed the tabs. There is no way to recover a deleted tab. Deleting a default tab has no impact on the dashboard for other user accounts.

**Procedure**
1. Go to the **Dashboard**.
2. Open the tab to delete.
3. Click the **X** next to the name of the tab.
4. Click **OK** to confirm.

The tab is deleted.

---

**Understanding Widgets**

Widgets are the core components for the dashboard. Tabs provide the layout and widgets provide the actual data for the dashboard.
Dashboard, Widgets, and Reports

**Note**
Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Download the Control Manager widget pool (under **Product programs and widget pool** on the **Manual Download** and **Scheduled Download** screens) periodically to check for new or updated widgets.

The data a widget displays comes from one of the following places:

- Control Manager database
- Trend Micro Smart Protection Network
- Managed products added to the Dashboard **Server Visibility** list

**Note**
Smart Feedback must be enabled to display data for widgets that include data from Smart Protection Network.

The data a widget displays is controlled in two ways:

**Table 4-1. Widget Data**

<table>
<thead>
<tr>
<th><strong>Item</strong></th>
<th><strong>Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User account</td>
<td>A user’s account grants or restricts access to any managed product registered to Control Manager.</td>
</tr>
<tr>
<td>Scope</td>
<td>The data scope on many widgets can be individually configured. This means a user can further specify the data source location for the widget. <strong>Example</strong>: An OfficeScan administrator, who manages multiple OfficeScan servers, could create one tab and add widgets that display data for only one OfficeScan server.</td>
</tr>
</tbody>
</table>
Adding Widgets to a Tab

After adding widgets to a tab, drag-and-drop the widgets to various locations within the tab. To customize widgets, see *Customizing Widgets on page 4-6*.

**Procedure**

1. Go to the **Dashboard** and then open the appropriate tab.

2. Click the **Add Widgets** at the upper right corner of the tab.

   The **Add Widgets** screen appears.

3. Do the following:
   - Click a category from the left and then select the check box next to the name of all applicable widgets that appear.
   - Use the search bar to select a specific widget.

4. Click **Add**.

All selected widgets are added to the tab.

Customizing Widgets

You can manually update, configure or filter the displayed widget information. It is also possible to display information about a specific time period. Some widgets represent the data in graph or table format.

For other customizations, see *Widget Options on page 4-7* or *Using Endpoint Encryption Widgets on page 4-8*.

**Procedure**

1. Go to the **Dashboard** and then open the appropriate tab.

2. Click the time link in the upper-left corner of the widget.
3. For some widgets, select the style to display information by clicking the chart or list icon in the upper right corner of the widget.

4. For some widgets, click the legend at the bottom of the widget to filter the information.

**Widget Options**

The following illustration and table provide a general overview of available widget options. Different widgets may have different options available.

**FIGURE 4-1. Widget Options**

**TABLE 4-2. Widget Option Descriptions**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The total number of objects (examples: events, devices, logs) that the widget gathers data about. Click the number to view additional information.</td>
</tr>
<tr>
<td>2</td>
<td>The information that the widget displays.</td>
</tr>
<tr>
<td>3</td>
<td>The Enterprise associated with the widget data.</td>
</tr>
<tr>
<td>4</td>
<td>The name of the widget. Change the name by clicking the icon to configure widget options.</td>
</tr>
<tr>
<td>5</td>
<td>Click the icon to configure the displayable options for that widget. Each widget has different configuration options.</td>
</tr>
</tbody>
</table>
Deleting Widgets

Procedure

1. Go to the Dashboard and then open the appropriate tab.
2. Click the icon in the upper right corner of the widget.

Note
For information about the available widget options, see Widget Options on page 4-7.

Using Endpoint Encryption Widgets

Control Manager has several Endpoint Encryption widgets to manage users, devices, and reports. The following widgets are available:

- Endpoint Encryption Users Widget on page 4-9
- Endpoint Encryption Devices Widget on page 4-11
- Full Disk Encryption Status Widget on page 4-13
The **Endpoint Encryption Users** widget provides user management capability directly from the Control Manager dashboard. Use the **Endpoint Encryption Users** widget to add or remove Endpoint Encryption user accounts, reset passwords, change permissions, configure policy group priority, import from Active Directory, and search for specific user accounts.

---

**Note**

For information about managing users with the **Endpoint Encryption Users** widget, see [Users in Control Manager on page 6-1](#).

For information about adding existing Endpoint Encryption users to a policy, see [Configuring Endpoint Encryption Users Rules on page 3-14](#).
**Figure 4-2. Endpoint Encryption Users Widget**

**Table 4-3. Endpoint Encryption Users Widget Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The total number of users in the entire Enterprise, selected policy, or specified search.</td>
</tr>
<tr>
<td>2</td>
<td>All users in the Enterprise, selected policy, or specified search.</td>
</tr>
<tr>
<td>3</td>
<td>Click the icon to filter which Endpoint Encryption users appear in the table.</td>
</tr>
<tr>
<td>4</td>
<td>Click the <strong>Show</strong> drop-down box to select the Enterprise or a specific policy to show in the table.</td>
</tr>
<tr>
<td>5</td>
<td>Use the search field to specify parameters to search against.</td>
</tr>
<tr>
<td>6</td>
<td>Click the icon to configure widget settings.</td>
</tr>
<tr>
<td>7</td>
<td>Click the icon to refresh widget data.</td>
</tr>
<tr>
<td>8</td>
<td>Click the icon to view online help.</td>
</tr>
<tr>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>9</td>
<td>Click the ☒ icon to close the widget.</td>
</tr>
<tr>
<td>10</td>
<td>View the last time that the widget synchronized data with PolicyServer.</td>
</tr>
<tr>
<td>11</td>
<td>Click the ⚒ icon to view user attributes or to perform actions on any selected user.</td>
</tr>
<tr>
<td>12</td>
<td>Click the 📜 icon to add individual users, import users from a CSV file, or import users from Active Directory LDAP.</td>
</tr>
</tbody>
</table>

**Endpoint Encryption Devices Widget**

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

The **Endpoint Encryption Devices** widget provides Endpoint Encryption device management capability directly from the Control Manager dashboard. Use the **Endpoint Encryption Devices** widget to monitor activity, search for Endpoint Encryption devices, or secure endpoint data by initiating lock or erase commands when an endpoint is lost or stolen.

---

**Note**

For information about managing devices with the **Endpoint Encryption Devices** widget, see *Devices in Control Manager on page 7-1*.

For information about adding Endpoint Encryption devices to a policy, see *Specifying Policy Targets on page 3-12*. 
FIGURE 4-3. Endpoint Encryption Devices Widget

TABLE 4-4. Endpoint Encryption Devices Widget Description

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View the total number of devices in the entire Enterprise, selected policy, or specified search.</td>
</tr>
</tbody>
</table>
| 2    | View all devices in the entire Enterprise, selected group, or specified search.  
  
  - **Device Name:** The computer name associated with the Endpoint Encryption device.  
  - **Agent:** The installed Endpoint Encryption agent.  
  - **FDE Encryption Status:** If Full Disk Encryption agent is installed, the encryption status. For information, see *Full Disk Encryption Status Widget on page 4-13*.  
  - **Status:** The current status of the Endpoint Encryption device. |
<p>| 3    | Click the icon to select the Endpoint Encryption agent and filter the devices shown in the table. |
| 4    | Click the Show drop-down box to select the entire Enterprise or a specific policy to show in the table. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Use the search field to specify parameters to search against. Any attributes listed in devices attributes can be searched.</td>
</tr>
<tr>
<td>6</td>
<td>Click the icon to configure widget settings.</td>
</tr>
<tr>
<td>7</td>
<td>Click the icon to refresh widget data.</td>
</tr>
<tr>
<td>8</td>
<td>Click the icon to view online help.</td>
</tr>
<tr>
<td>9</td>
<td>Click the icon to close the widget.</td>
</tr>
<tr>
<td>10</td>
<td>View the last time that the widget synchronized data with PolicyServer.</td>
</tr>
<tr>
<td>11</td>
<td>Click the icon to view device attributes or to perform actions on the selected device.</td>
</tr>
</tbody>
</table>

**Full Disk Encryption Status Widget**

The **Full Disk Encryption Status** widget shows the current encryption status of any Endpoint Encryption in the Enterprise.

![Full Disk Encryption Status Widget](image)

**Figure 4-4. Full Disk Encryption Status Widget**
### TABLE 4-5. Full Disk Encryption Status Widget Description

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Status  | The status of the Endpoint Encryption device. Statuses include:  
  - **Encrypted**: The Endpoint Encryption device is 100% encrypted.  
  - **Encrypting**: The Endpoint Encryption device is currently encrypting the hard disk. The status changes to “Fully Encrypted” once encryption completes and the endpoint restarts.  
  - **Not encrypted**: The Endpoint Encryption device is 0% encrypted.  
  - **Decrypting**: The Endpoint Encryption device is currently decrypting the hard disk. The status changes to Not Encrypted once the decryption completes and the endpoint restarts.  
  - **Unknown**: The Endpoint Encryption device synchronized, but PolicyServer cannot determine the encryption status. |
| Rate    | The percentage that the Endpoint Encryption device is encrypted. |
| Devices | The number of Endpoint Encryption devices with that current status. Click the number to view the Endpoint Encryption Devices report. For more information, see *Full Disk Encryption Status Report* on page 4-14. |

---

**Note**

At the bottom of the widget, click the number next to **Total** to view the Endpoint Encryption Status report. For more information, see *Full Disk Encryption Status Report* on page 4-14.

### Full Disk Encryption Status Report

The following table describes the **Full Disk Encryption Status** report. Use it to understand how to read the report details.
### Table 4-6. Full Disk Encryption Status Report Example

<table>
<thead>
<tr>
<th><strong>Header</strong></th>
<th><strong>Example</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>GP1</td>
<td>The title of the policy controlling the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>TREND-4136D2DB3</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device ID</td>
<td>1fabfbff-0001-06e5-000c-297085710000</td>
<td>The unique ID established after the Endpoint Encryption agent was installed on the endpoint and a new Endpoint Encryption device was registered with PolicyServer.</td>
</tr>
<tr>
<td>Application</td>
<td>Full Disk Encryption</td>
<td>The currently installed Endpoint Encryption agent.</td>
</tr>
<tr>
<td>Status</td>
<td>Not Encrypted</td>
<td>The current state of the Endpoint Encryption device. For an encryption status list, see <em>Full Disk Encryption Status Widget on page 4-13</em>.</td>
</tr>
<tr>
<td>Last Synchronized Date</td>
<td>10/07/2013 11:05 am</td>
<td>The timestamp when the Endpoint Encryption device last updated policies from PolicyServer.</td>
</tr>
<tr>
<td>Last Policy Enforcement</td>
<td>10/07/2013 11:05 am</td>
<td>The timestamp when the Control Manager last enforced policy changes on PolicyServer.</td>
</tr>
</tbody>
</table>
Endpoint Encryption Unsuccessful Device Logon Widget

The **Endpoint Encryption Unsuccessful Device Logon** widget shows all Endpoint Encryption devices that had unsuccessful logon attempts by any user (Endpoint Encryption user or non-Endpoint Encryption user). Unsuccessful device logon events may represent a security breach or the Endpoint Encryption user may have forgotten the logon credentials.

### Table 4-7. Endpoint Encryption Unsuccessful Device Logon widget column descriptions

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>The computer name of the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Policy</td>
<td>The policy managing the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Events</td>
<td>The number of logon attempts. Click the number to view the <strong>Endpoint Encryption Unsuccessful Device Logon</strong> report.</td>
</tr>
</tbody>
</table>
### Endpoint Encryption Unsuccessful Device Logon Report

The following table explains the **Endpoint Encryption Unsuccessful Device Logon** report. Use it to understand how to read the report details.

**Table 4-8. Endpoint Encryption Unsuccessful Device Logon Example**

<table>
<thead>
<tr>
<th><strong>Header</strong></th>
<th><strong>Example</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Policy</td>
<td>GP1</td>
<td>The title of the policy controlling the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>TRENDS-4136D2DB3</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device ID</td>
<td>1fabfbff-0001-06e5-000c-297085710000</td>
<td>The unique ID established after the Endpoint Encryption agent was installed on the endpoint and a new Endpoint Encryption device was registered with PolicyServer.</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.152.219</td>
<td>The Endpoint Encryption device IP address.</td>
</tr>
<tr>
<td>Application</td>
<td>Full Disk Encryption</td>
<td>The currently installed Endpoint Encryption agent.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Mary Jones</td>
<td>The first and last name of the Endpoint Encryption user account. If the specified user name is not a valid Endpoint Encryption user name, the column shows “Not Recorded”.</td>
</tr>
<tr>
<td>Event</td>
<td>Unsuccessful Fixed Password Login</td>
<td>The logged event including the authentication method.</td>
</tr>
</tbody>
</table>
Endpoint Encryption Unsuccessful User Logon Widget

The **Endpoint Encryption Unsuccessful User Logon** widget shows all attempts by any user (Endpoint Encryption user or non-Endpoint Encryption user) to log on to any Endpoint Encryption device.

![Endpoint Encryption Unsuccessful User Logon Widget](image)

**Figure 4-5. Endpoint Encryption Unsuccessful User Logon Widget**

**Table 4-9. Endpoint Encryption Unsuccessful User Logon Widget Description**

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name used to attempt to log on to the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Display Name</td>
<td>The display name of the user account that attempted to log on to the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Events</td>
<td>The number of authentication attempts. Click the number to view the Endpoint Encryption Unsuccessful User Logon report.</td>
</tr>
</tbody>
</table>
Endpoint Encryption Unsuccessful User Logon Report

The following table explains the **Endpoint Encryption Unsuccessful User Logon** report. Use it to understand how to read the report details.

**Table 4-10. Endpoint Encryption Unsuccessful User Logon Report Example**

<table>
<thead>
<tr>
<th><strong>HEADER</strong></th>
<th><strong>EXAMPLE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Policy</td>
<td>GP1</td>
<td>The title of the policy controlling the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>TRENDS-4136D2DB3</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device ID</td>
<td>1fabfbbff-0001-06e5-00c-297085710000</td>
<td>The unique ID established after the Endpoint Encryption agent was installed on the endpoint and a new Endpoint Encryption device was registered with PolicyServer.</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.152.219</td>
<td>The Endpoint Encryption device IP address.</td>
</tr>
<tr>
<td>Application</td>
<td>Full Disk Encryption</td>
<td>The currently installed Endpoint Encryption agent.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Mary Jones</td>
<td>The first and last name of the Endpoint Encryption user account. If the specified user name is not a valid Endpoint Encryption user name, the column shows “Not Recorded”.</td>
</tr>
<tr>
<td>Event</td>
<td>Unsuccessful Fixed Password Login</td>
<td>The logged event including the authentication method.</td>
</tr>
</tbody>
</table>

**Endpoint Encryption Device Lockout Widget**

The **Endpoint Encryption Device Lockout** widget shows Endpoint Encryption devices that are locked out due to policy restrictions.
Note

For information about Endpoint Encryption device lockout rules, see *Account Lockout and Device Lock Actions on page 3-22.*

![Figure 4-6. Endpoint Encryption Device Lockout Widget](image)

**Table 4-11. Endpoint Encryption Device Lockout Widget Description**

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Policy</td>
<td>The title of the policy controlling the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Lockout</td>
<td>The timestamp when PolicyServer issued the device lock command. The Endpoint Encryption device does not actually lock until after the Endpoint Encryption agent synchronizes policies with PolicyServer.</td>
</tr>
<tr>
<td>Details</td>
<td>Click details icon to view the Endpoint Encryption Device Lockout report.</td>
</tr>
</tbody>
</table>

At the bottom of the widget, click the number next to **Total** to view the report.
Endpoint Encryption Device Lockout Report

The following table explains the Endpoint Encryption Device Lockout report. Use it to understand how to read the report details.

---

**Note**

For information about account lockout and device lock actions, see *Account Lockout and Device Lock Actions on page 3-22.*

---

**TABLE 4-12. Endpoint Encryption Device Lockout Report Example**

<table>
<thead>
<tr>
<th>HEADER</th>
<th>EXAMPLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Policy</td>
<td>GP1</td>
<td>The title of the policy controlling the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>TREND-4136D2DB3</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Device ID</td>
<td>1fabfbff-0001-06e5-000c-297085710000</td>
<td>The unique ID established after the Endpoint Encryption agent was installed on the endpoint and a new Endpoint Encryption device was registered with PolicyServer.</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.152.219</td>
<td>The Endpoint Encryption device IP address.</td>
</tr>
<tr>
<td>Application</td>
<td>Full Disk Encryption</td>
<td>The currently installed Endpoint Encryption agent.</td>
</tr>
<tr>
<td><strong>HEADER</strong></td>
<td><strong>EXAMPLE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display Name</td>
<td>Mary Jones</td>
<td>The first and last name of the Endpoint Encryption user account. If the specified user name is not a valid Endpoint Encryption user name, the column shows “Not Recorded”.</td>
</tr>
<tr>
<td>Event</td>
<td>Locked device due to invalid login attempt violation.</td>
<td>The logged event including the authentication method.</td>
</tr>
</tbody>
</table>

**Endpoint Encryption Security Violations Report Widget**

The **Endpoint Encryption Security Violations Report** widget shows the security violations assessed by the following reports:

- **Endpoint Encryption Consecutive Unsuccessful Device Logon**
- **Endpoint Encryption Policy Tampering**
- **Endpoint Encryption Log Integrity**

Generating a report gathers all security violations currently logged by PolicyServer. Once generated, click the number on the **Reports** column to view generated reports for that violation.

![Endpoint Encryption Security Violations Report Widget](image)

**Figure 4-7. Endpoint Encryption Security Violations Report Widget**
### Table 4-13. Endpoint Encryption Security Violations Report Description

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violation report type</td>
<td>The available report types for various violations.</td>
</tr>
<tr>
<td>Action</td>
<td>Click Generate to create a new report.</td>
</tr>
<tr>
<td>Reports</td>
<td>The total number of generated reports for that violation. Click the number to view available reports.</td>
</tr>
</tbody>
</table>

### Endpoint Encryption Consecutive Unsuccessful Device Logon Report

The following table explains the Endpoint Encryption Consecutive Unsuccessful Device Logon report. Use it to understand when the logon attempt occurred, the affected Endpoint Encryption device, and how many times the user attempted to log on to the Endpoint Encryption device.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Device Name</td>
<td>TREND-4136D2DB3</td>
<td>The computer name used by the Endpoint Encryption device.</td>
</tr>
<tr>
<td>Attempts</td>
<td>5</td>
<td>The number of times that a user attempted to log on to the Endpoint Encryption device.</td>
</tr>
</tbody>
</table>

### Endpoint Encryption Policy Tampering Report

The following table explains the Endpoint Encryption Policy Tampering report. Use it to understand how to read the report details.
TABLE 4-15. Endpoint Encryption Policy Tampering Report Example

<table>
<thead>
<tr>
<th>Header</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Event</td>
<td>Policy Value Integrity Check</td>
<td>Failed</td>
</tr>
<tr>
<td></td>
<td>Failed</td>
<td>The logged event including the authentication method.</td>
</tr>
</tbody>
</table>

Endpoint Encryption Log Integrity Report

The following table explains the **Endpoint Encryption Log Integrity** report. Use it to understand how to read the report details.

TABLE 4-16. Endpoint Encryption Log Integrity Report Example

<table>
<thead>
<tr>
<th>Header</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Timestamp</td>
<td>07/02/2012 01:56 pm</td>
<td>When the event occurred.</td>
</tr>
<tr>
<td>Event</td>
<td>Audit Log Record Missing</td>
<td>The logged event including the authentication method.</td>
</tr>
</tbody>
</table>

Chapter 5

Policies in Control Manager

This chapter explains how to use policies and provides detailed information about individual policy setting values.

Topics include:

• Groups on page 5-2
• Understanding Policies on page 5-2
• Understanding Policy Types on page 5-3
• Understanding Policy Target Settings on page 5-6
• Understanding the Managed Server List on page 5-26
• Updating the Policy Templates on page 5-31
Groups

To streamline policy management, Control Manager merges the PolicyServer MMC group and policy hierarchy together. PolicyServer maintains the same policy and group configuration no matter which management console you prefer. When you create a new policy target in Control Manager, PolicyServer MMC shows a new group that contains the policy configurations and the users added to that policy.

Important
Control Manager always takes precedence. Any modifications to the group assignment in PolicyServer MMC are automatically overwritten the next time that Control Manager synchronizes with PolicyServer.

Understanding Policies

Policy management allows administrators to enforce product settings on managed products and endpoints from a single management console. Administrators create a policy by selecting the targets and configuring a list of product settings.

Control Manager policies have the following attributes:

Table 5-1. Control Manager Policy Options

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>The name of the policy configuration.</td>
</tr>
<tr>
<td>Targets</td>
<td>Administrators can manually select targets or use a filter to automatically assign targets to their policies. The target selection method determines the policy type and how the policy works. See Understanding Policy Types on page 5-3 for more information about policy types. To include a managed product or endpoint as the target, make sure the product version of the managed product or endpoint supports policy management in Control Manager. The Policy Template Settings screen contains information about supported product versions.</td>
</tr>
</tbody>
</table>
ACTIONS

Settings

Once Control Manager deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Control Manager enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Control Manager enforces the policy settings.

**Note**

Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period.

Administrators can use the **Policy Management** screen to perform the following tasks:

- *Creating a Policy* on page 3-10
- *Editing a Policy* on page 5-24
- *Deleting a Policy* on page 5-25
- *Copying Policy Settings* on page 5-23

**Note**

Make sure to use the **Product Directory** to move the managed PolicyServer instance from the New Entity folder to the Endpoint Encryption folder in the Product Directory. For more information, see *Understanding the Product Directory* on page A-15.

---

**Understanding Policy Types**

Control Manager provides three types of policies administrators can create. Each policy type differs in the target selection method, which affects how a policy works. The policy list arranges the policy types in the order as described in the following table.
### Table 5-2. Policy Types

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Specified   | Uses the search or browse function to locate specific targets and manually assigns them to the policy  
|             | Uses when administrators plan to deploy specific settings only to a certain targets  
|             | Remains static on the top of the policy list and takes priority over any filtered policies |
| Filtered    | Uses a filter to automatically assign current and future targets to the policy  
|             | Useful for deploying standard settings to a group of targets  
|             | Administrators can change the priority of filtered policies in the policy list  
|             | See Assigning Endpoints to Filtered Policies on page 5-4 for more information on how Control Manager assign targets to filtered policies |
| Draft       | Allows administrators to save policy settings as a draft without selecting any targets. Control Manager saves draft policies with the lowest priority at the bottom of the list. |

### Assigning Endpoints to Filtered Policies

When a new endpoint registers to Control Manager, it goes through the filtered policies in the list in descending order. Control Manager assigns the new endpoint to a filtered policy when the following conditions are both satisfied:
• The new endpoint matches the target criteria in the policy
• The policy creator has the permission to manage the new endpoint

The same action applies to an endpoint already assigned to a policy, but the policy creator later deletes the policy.

---

**Note**

For endpoints just registered to Control Manager and for those just released from deleted policies, there is a three-minute grace period during which no endpoint allocation occurs. These endpoints are temporarily without policies during this period.

---

If an endpoint does not meet the target criteria in any filtered policies, the endpoint does not associate with any policies. Control Manager allocates these endpoints again when the following actions occur:

• Create a new filtered policy
• Edit a filtered policy
• Reorder the filtered policies
• Daily endpoint allocation schedule

Control Manager uses a daily endpoint allocation schedule to ensure that endpoints are assigned to the correct policies. This action occurs once at 3:15 pm every day. When endpoint properties change, such as the operating system or IP address, these endpoints require the daily schedule to re-assign them to the correct policies.

---

**Note**

If the endpoints are offline during the daily endpoint allocation schedule, the policy status for these endpoints will remain pending until they go online.

---

When the above actions occur, Control Manager allocate endpoints based on the following conditions:
### Table 5-3. Endpoint Allocation for Filtered Policies

<table>
<thead>
<tr>
<th>Action</th>
<th>New endpoints or endpoints from deleted policies</th>
<th>Endpoints without policies</th>
<th>Endpoints with policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit a policy</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reorder the filtered policies</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Daily endpoint allocation schedule</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

### Understanding Policy Target Settings

This section explains how to use various windows to change a policy, but does not explain the process to modify every policy. All policies have default values. The PolicyServer MMC has a common set of windows to use when modifying a policy. One policy will have an editor window available to edit the numbers, ranges and values associated with the policy while another policy will have a window to modify text strings.

When managing policies, note the following:

- Policies are configurable by application within each group.
- Policy inheritance only occurs when a subgroup is created. For information about group permissions, see *About Groups on page 10-2*.

### Understanding the Policy List

The policy list displays the information and status of policies created by all users. When a new endpoint registers to Control Manager, it goes through the filtered policies in the list in descending order. Control Manager assigns the new endpoint to a filtered policy when the following conditions are both satisfied:
The new endpoint matches the target criteria of the policy
- The policy creator has the permission to manage the new endpoint

The following table describes the items in the policy list.

**Table 5-4. Policy List**

<table>
<thead>
<tr>
<th><strong>MENU ITEM</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Priority      | Displays the priority of the policies.  
|               | • Control Manager lists policies from the highest to the lowest priority.  
|               | • When administrators create a filtered policy, Control Manager saves the new policy as the lowest priority policy.  
|               | • A specified policy takes priority over any filtered policies and remains on the top of the list. Administrators cannot reorder specified policies.  
|               | • Control Manager places draft policies at the bottom of the list. |
| Policy        | Displays the name of the policy. |
| Targets       | Displays how administrators select targets for the policy.  
|               | • Specified: Uses the browse or search function to select specific targets for the policy. Specified policies remain static on the top of the policy list and take priority over filtered policies.  
|               | • Filtered: Uses a filter to automatically assign current and future endpoints to the policy. Administrators can rearrange the priority of filtered policies.  
<p>|               | • None: The policy creator saved the policy as a draft without selecting any targets. |
| Deployed      | Displays the number of targets that have applied the policy settings. |</p>
<table>
<thead>
<tr>
<th><strong>Menu Item</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Displays the number of targets that have not applied the policy settings. Click the pending number to check the policy status.</td>
</tr>
<tr>
<td>Creator</td>
<td>Displays the user who created the policy.</td>
</tr>
<tr>
<td>Endpoints/Products without policies</td>
<td>Displays the number of managed products or endpoints to which Control Manager has not assigned a policy.</td>
</tr>
<tr>
<td>Total endpoints/products</td>
<td>Displays the number of managed products or endpoints available for policy management.</td>
</tr>
</tbody>
</table>

**Note**
The numbers in Deployed, Pending, Endpoints/Products without policies, and Total endpoints/products only reflect the endpoints or managed products an administrator has the permissions to manage.

## Creating a Policy

The following procedure explain how to configure a Control Manager policy that affects Endpoint Encryption users and devices.

**Important**
To add a user account to the policy, make sure that the user account already exists.

**Note**
For information about available policy settings, see *Endpoint Encryption Policy Settings on page 5-12*.

For information about adding new Endpoint Encryption users, see *Adding Users to Endpoint Encryption on page 6-4*.

For information about configuring Active Directory, see the *Endpoint Encryption Installation and Migration Guide*.

For information about policy mapping between Control Manager and PolicyServer MMC, see *Policy Mapping Between Management Consoles on page D-1*.
Procedure

1. Go to Policies > Policy Management.
2. From the Product drop-down list, select Endpoint Encryption.
3. Click Create.

The Create Policy screen appears.

4. Specify a policy name.
5. Select one of the following policy target options:
   - **None (Draft Only):** Create a policy with no targets (endpoints)
   - **Filter by Criteria:** Endpoint Encryption does not support filtering by criteria
   - **Specify Target(s):** Specify existing endpoints.

**Note**

For more information about policy targets, see *Specifying Policy Targets on page 3-12*
   
   - Configure **User** policies.
     See *Configuring Endpoint Encryption Users Rules on page 3-14*.
   
   - Configure **Full Disk Encryption** policies.
     See *Configuring Full Disk Encryption Rules on page 3-15*.
   
   - Configure **File Encryption** policies.
     See *Configuring File Encryption Rules on page 3-17*.
   
   - Configure **Common** policies.
     See *Configuring Common Policy Rules on page 3-19*.

7. Click **Save**.

---

**Specifying Policy Targets**

Use the **Specify Target(s)** screen to assign Endpoint Encryption devices to the policy.

---

**Note**

The **Specify Target(s)** screen is available when creating a new policy. For information about creating a policy, see *Creating a Policy on page 3-10*. 

---
Procedure

1. From the Specify Target(s) screen, click the Browse tab.

2. From the left pane, expand the tree to select the managed folder.
   
   Example: CM-PI-2K8 > Local Folder > TMEE > TMEE > QA2

3. Select any appropriate Endpoint Encryption devices, or select the top check box to select all Endpoint Encryption devices listed on the current page.

4. Click Add Selected Targets.

**Note**

To immediately select all devices in the managed folder, click Add All from Selected Folder.

“View Action List” and “View Results” update based on the selection.
5. Click OK.

Endpoint Encryption Policy Settings

Configuring Endpoint Encryption Users Rules

The following procedure explains the configurable options for policy rules affecting authentication and Endpoint Encryption user accounts.

Procedure

1. Create a new Endpoint Encryption policy.
   
   See *Creating a Policy on page 3-10*.

2. Click **Users**.

   The **Users** policy rules settings appear.

   ![Figure 5-2. Endpoint Encryption Users Policy Rules](image)

3. Under **Domain User Settings**, select **Enable domain authentication** to specify whether users require domain authentication.
Important

Active Directory (AD) synchronization requires PolicyServer to have three enabled components:

a. Configure the AD domain.

b. Configure the policy group to point to the proper Organizational Unit (OU).

c. Configure the policy group with appropriate credentials to access the AD domain that matches the policy group's “Distinguished Name”.

To configure domain authentication, see PolicyServer Active Directory Synchronization in the Endpoint Encryption Installation and Migration Guide.

4. Under User Management, configure user access.

- Select All Endpoint Encryption users to allow all users, domain and local accounts, to authenticate Endpoint Encryption devices.

- Select Select specific users to specify which already added Endpoint Encryption users can authenticate to managed endpoints.

Note

Policy rules only affect existing user accounts. Before configuring policies, add new users with the Endpoint Encryption Users Widget. For more information, see Adding Users to Endpoint Encryption on page 6-4.

Configuring Full Disk Encryption Rules

The following procedure explains the configurable options for policy rules affecting Full Disk Encryption devices.

Note

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.
Procedure

1. Create a new Endpoint Encryption policy.
   See *Creating a Policy on page 3-10*.

2. Click **Full Disk Encryption**.
   The **Full Disk Encryption** policy rules settings appear.

   ![Figure 5-3. Full Disk Encryption Policy Rules](image)

   **Figure 5-3. Full Disk Encryption Policy Rules**

3. Under **Encryption**, select **Encrypt device** to start full disk encryption when the Endpoint Encryption agent synchronizes policies with PolicyServer.

   **WARNING!**
   Do not deploy encryption to Full Disk Encryption agents without first preparing the endpoint's hard drive.

   For information about preparing the hard drive, see *Full Disk Encryption Deployment Outline* in the *Endpoint Encryption Installation Guide*.

4. Under **Agent Settings**, select the following options:
• Select **Bypass Full Disk Encryption Preboot** to allow the user to authenticate directly into Windows without protection from preboot authentication.

• Select **Users are allowed to access system recovery utilities on the device** to allow the user to access the Recovery Console.

For information about configurable options and available tools in Full Disk Encryption, see *Full Disk Encryption Recovery Console on page 14-20.*

5. Under **Notifications**, configure the following options:

• Select **If found, display the following message on the device** to show a message when the *If Found* policy is active.

• Select **Display Technical Support contact information** to show a message after the user logs on to the Full Disk Encryption agent.

• Select **Show a legal notice** to show the specific legal message at start up or only after installing the Full Disk Encryption agent.

---

### Configuring File Encryption Rules

The following procedure explains the configurable options for policy rules affecting File Encryption devices.

**Procedure**

1. Create a new Endpoint Encryption policy.

   See *Creating a Policy on page 3-10.*

2. Click File Encryption.
The **File Encryption** policy rules settings appear.

**Figure 5-4. File Encryption Policy Rules**

3. Under **Folder to Encrypt**, specify folders that are automatically created and encrypted on the endpoint when the File Encryption agent synchronized policies.

4. Under **Encryption Key**, select the encryption for the File Encryption encrypted folder.
   - **User key**: Use a unique key for each Endpoint Encryption user. Only the Endpoint Encryption user can decrypt files that he or she encrypted.
• **Policy key**: Use a unique key for each policy. Only Endpoint Encryption users and devices in the policy can decrypt files.

• **Enterprise key**: Any Endpoint Encryption user or device in the Enterprise can decrypt the files.

---

**Note**

Selecting **Policy key** or **Enterprise key** controls the sharing for the File Encryption shared key. For more information, see *File Encryption Shared Key Encryption on page 13-15*.

---

5. Under **Storage Devices**, configure the following options:

• Select **Disable optical drives** to control whether removable media is accessible from the endpoint.

• Select **Disable USB drives** to control when the USB ports are disabled. Options are:
  • **Always**
  • **Logged out**
  • **Never**

• Select **Encrypt all files and folders on USB devices** to automatically encrypt all the files and folders on removable drives when plugged into the endpoint.

• Select **Specify the file path to encrypt on USB devices** to add or remove encrypted folders to USB drives. If a folder does not exist, it is created. If no drive letter is specified, all USB devices are affected.

6. Under **Notifications**, select **Show a legal notice** to show the specific legal message at start up or only after installing the File Encryption agent.

---

**Configuring Common Policy Rules**

This section explains the configurable options for policy rules affecting all Endpoint Encryption devices.
Procedure

1. Create a new Endpoint Encryption policy.
   
   See *Creating a Policy on page 3-10*.

2. Click **Common**.
   
   The **Common** policy rules settings appear.

3. Under **Allow User to Uninstall**, select **Allow User (non-administrator) accounts to uninstall agent software** to allow any Endpoint Encryption user to uninstall the agent.
Note
By default, only Enterprise Administrator accounts can uninstall Endpoint Encryption agents.

4. Under **Lockout and Lock Device Actions**, configure the following options:

   - Select **Lock account after <number> days** to specify the number of days that the Endpoint Encryption device locks if it does not synchronize policies.

   - Use **Account lockout action** to specify whether the remote authentication or erase action occurs at lockout.

   **Note**
   For information about lock options, see *Account Lockout and Device Lock Actions on page 3-22*

   - Select **Failed log on attempts allowed** to specify how many times that a user can attempt to authenticate before the Endpoint Encryption device locks.

   - For Full Disk Encryption or File Encryption devices, separately configure the following:

     - Use **Device locked action** to specify whether the “Remote Authentication” or the “Erase” action occurs at lockout.

   **Note**
   For information about lock options, see *Account Lockout and Device Lock Actions on page 3-22*

   - Use **Number of minutes to lock device** to specify the duration that time delay locks the Endpoint Encryption device from authentication

5. Under **Password**, configure the following options:

   - Select **Users must change password after <number> days** to control when a user is prompted to update password.
• Select **Users cannot reuse the previous <number> passwords** to specify how many previous passwords the user may reuse.

• Select **Number of consecutive characters allowed in a password** to specify how many repeated characters a user may specify in the password.

• Select **Minimum length allowed for passwords** to specify how many characters the user is required to use in the password.

6. Under **Password Requirements**, specify the password character limitations.

   • Letters
   • Lowercase characters
   • Uppercase characters
   • Numbers
   • Symbols

---

**Important**

The sum total of letters, numbers, and symbols cannot exceed 255 characters.

---

**Account Lockout and Device Lock Actions**

Some policies have settings to lock out a user account or to lock a device based on certain criteria. Account lockout and device lock actions affect the Endpoint Encryption device whether or not the agent synchronizes policies with PolicyServer. For example, if the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time, the Endpoint Encryption agent automatically locks the Endpoint Encryption device. Use the tables below to understand the actions available for the account lockout and device lock actions.

**Table 5-5. Account Lockout Actions**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote authentication</td>
<td>Users cannot log on to the Endpoint Encryption device until after Technical Support provides remote authentication assistance.</td>
</tr>
</tbody>
</table>
**ACTION** | **DESCRIPTION**
---|---
Erase | All data is erased the next time that the agent synchronizes policies.

**Note**
Account lockout actions take effect when the Endpoint Encryption agent does not communicate with PolicyServer for a certain period of time (set by policy).

**TABLE 5-6. Device Lock Actions**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase</td>
<td>All data is erased the next time that the Endpoint Encryption agent synchronizes policies.</td>
</tr>
<tr>
<td>Remote authentication</td>
<td>Users cannot log on to Endpoint Encryption devices until after Technical Support provides remote authentication assistance.</td>
</tr>
<tr>
<td>Time delay</td>
<td>Users cannot log on to Endpoint Encryption devices for a specified time duration.</td>
</tr>
</tbody>
</table>

**Note**
Device lock actions take effect when the Endpoint Encryption user has too many unsuccessful logon attempts to that Endpoint Encryption device (set by policy).

**Remote Help Policy Rules**

The following table describes the locations of the account lockout and device lock policies that affect Remote Help authentication. Use it to understand which policies are appropriate to set.
TABLE 5-7. Remote Help Policy Locations

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Policy Server MMC Menu Path</th>
<th>Control Manager MMC Menu Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Action</td>
<td>Login &gt; Account Lockout Action</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Account Lockout Action</td>
<td>The action taken when the length of time in “Account Lockout Actions” include: erase, remote authentication.</td>
</tr>
<tr>
<td>Account Lockout Period</td>
<td>Login &gt; Account Lockout Period</td>
<td>Common &gt; Lockout and Lock Device Actions &gt; Lock account after [ ] days</td>
<td>The number of days that a device can not communicate with PolicyServer before “Account Lockout Action” is called.</td>
</tr>
<tr>
<td>Device Locked Action</td>
<td>For each agent: Login &gt; Device Locked Action</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Device locked action</td>
<td>The action taken when the &quot;Failed Attempts Allowed” policy value has been exceeded. Actions include: time delay, erase, remote authentication.</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>For each agent: Login &gt; Failed Login Attempts Allowed</td>
<td>For each agent: Common &gt; Lockout and Lock Device Actions &gt; Failed logon attempts allowed</td>
<td>The number of failed login attempts allowed before executing the action defined in “Device Locked”.</td>
</tr>
</tbody>
</table>

Changing Setting Permissions

When configuring the policy settings, administrators can grant managed product administrators the permissions to define the settings of certain features. Follow the steps below to change setting permissions when creating or editing a policy:
Procedure

1. In the Settings section, click **Show Permissions**. A switch appears at the right side of each feature.

2. Click the switch to change the setting permission.
   - **Centrally Managed** (Blue): The assigned targets will comply to the settings defined in the policy.
   - **Locally Managed** (Orange): Control Manager does not deploy the settings of the selected feature to the targets. The managed product administrators can define the settings through the product console.

**Note**

When administrators deploy a policy with all feature settings switched to locally managed, the policy status of the targets will remain in the pending state.

Copying Policy Settings

Administrators can copy the settings from an existing policy, create a new policy with the same settings, and deploy the settings to different endpoints or managed products.

Procedure

1. Navigate to **Policies > Policy Management**.
The Policy Management screen appears.

2. Select the type of product settings from the Product list.

The screen refreshes to display policies created for the selected managed product.

3. Select a policy from the list.

4. Click Copy Settings.

The Copy and Create Policy screen appears.

5. In the Policy Name field, type a name for the policy.

6. Assign Targets to the policy.

7. Click Deploy.

---

**Note**

- After clicking Deploy, please wait two minutes for Control Manager to deploy the policy to the targets. Click Refresh on the Policy Management screen to update the status information in the policy list.

- Control Manager enforces the policy settings on the targets every 24 hours.

---

**Editing a Policy**

Administrators can change the information of a policy including the policy name, targets, and settings. Only the policy creator can modify the policy.

Control Manager supports the following changes:

- Modifying a filtered policy
- Adding more targets to a specified policy
- Removing some targets from a specified policy
Policies in Control Manager

Note
Control Manager only allows the policy creators to make changes to their own policies. However, the root account can edit every policy in the list.

Procedure

1. Go to Policies > Policy Management.

The Policy Management screen appears.

2. Select the type of product settings from the Product list.

The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the Policy column.

The Edit Policy screen appears.

4. Modify the policy.

5. Click Deploy.

The changes apply immediately.

Note

• After clicking Deploy, please wait two minutes for Control Manager to deploy the policy to the targets. Click Refresh on the Policy Management screen to update the status information in the policy list.

• Control Manager enforces the policy settings on the targets every 24 hours.

Deleting a Policy

Administrators can remove a policy from the list. Control Manager then re-allocates the targets associated with the deleted policy if the targets match the filtering criteria of another policy. Those without a match become endpoints without policies, and they keep the settings defined by the deleted policy unless a managed product administrator modifies the settings.
Control Manager only allows the policy creator to delete his own policies. However, the root account can delete every policy in the list.

Procedure

1. Navigate to Policies > Policy Management.
   
The Policy Management screen appears.

2. Select the type of product settings from the Product list.
   
The screen refreshes to display policies created for the selected managed product.

3. Select the policy to delete.

4. Click Delete.
   
   A confirmation screen appears.

5. Click OK.

Understanding the Managed Server List

The Managed Servers screen shows the servers administrators can manage using policy management. Use the screen to add and edit managed products that do not have MCP agents.

When the Add button is disabled, policy management only supports managed products using MCP agents.

For managed products using MCP agents, Control Manager uses the Single Sign-on (SSO) function to access these products by default. Administrators can edit the authentication information for the following reasons:

- The SSO function does not function properly
• Administrators want to access the managed product using another account

**TABLE 5-8. Managed Server List**

<table>
<thead>
<tr>
<th><strong>Menu Item</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Displays the server name of the managed product.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Displays the server display name of the managed product.</td>
</tr>
<tr>
<td>Product</td>
<td>Displays the name of the managed product.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Displays how the managed product registers to Control Manager.</td>
</tr>
<tr>
<td></td>
<td>• Automatic: The managed product registers to Control Manager through an MCP agent.</td>
</tr>
<tr>
<td></td>
<td>• Manual: Administrators manually added the managed product to the Managed Servers screen.</td>
</tr>
<tr>
<td>Last Report</td>
<td>Shows the date and time when Control Manager received a response from the managed product.</td>
</tr>
<tr>
<td>Actions</td>
<td>• Edit: Click this icon to update the server information.</td>
</tr>
<tr>
<td></td>
<td>• Delete: Click this icon to delete a manually added server.</td>
</tr>
</tbody>
</table>

**Note**

Control Manager cannot remove servers registered using MCP agents.

---

**Adding PolicyServer as a Managed Product to Control Manager**

Endpoint Encryption allows administrators to use Trend Micro Control Manager to control PolicyServer and manage Endpoint Encryption agent policies or use Trend Micro OfficeScan to deploy Endpoint Encryption agent software on managed endpoints.
To use Control Manager to manage PolicyServer, you must add PolicyServer as a managed product.

Make sure to complete the following tasks before proceeding:

1. Install and configure Control Manager.
   See the supporting documentation at:
2. Install and configure PolicyServer.
   See the *Endpoint Encryption Installation and Migration Guide*.

**Important**

Endpoint Encryption supports only one configured PolicyServer instance in Control Manager at a time. It is not possible to add multiple PolicyServer configurations. To configure a different PolicyServer, first remove the previously configured PolicyServer.

**Procedure**

1. Review all system requirements for compatible product versions.
   See the *Endpoint Encryption Installation and Migration Guide*.
2. Log on to Control Manager.
   The Managed Servers screen appears.
4. In the Server Type drop-down list, select Endpoint Encryption.
5. Click Add.
The **Add Server** screen appears.

![Add Server screen](image)

6. Specify **Server Information** options.
   - **Server**: Specify the PolicyServer host name and the port number. Use the following format:
   
   \[ \text{http(s)://<server_name>:port_number} \]

   **Note**
   
   Control Manager communicates with PolicyServer Endpoint Encryption Service. The default port number is 8080.

   - **Display name**: Specify how PolicyServer shows in the **Managed Servers** screen

7. Under **Authentication**, specify the user name and password of the Endpoint Encryption Enterprise Administrator account.

8. Under **Connection**, select **Use a proxy server for the connection** if PolicyServer requires a proxy connection.

9. Click **Save**.
Synchronization between Control Manager and PolicyServer may require several minutes to complete.

PolicyServer is added as a new managed product to Control Manager.

**Editing a Server**

**Procedure**

   
   The Managed Servers screen appears.

2. Click the Edit icon in the Actions column.

3. Edit the server information.

4. Click Save.

**Configuring the Proxy Settings**

Use a proxy server to connect to the managed products.

**Procedure**

   
   The Managed Servers screen appears.

2. Click Proxy Settings.
3. Select the protocol:
   - HTTP
   - SOCKS 5

4. Type the server name in the Server field.

5. Type the port number in the Port field.

6. Type the user name and password to access the server if it requires authentication.

7. Click Save.

---

**Updating the Policy Templates**

The **Policy Template Settings** screen lists the following components available for administrators to enable or upgrade:

- Policy Management Framework: The overall policy structure
- Product Support: The setting templates for managed products and endpoints
To check the product versions that support policy management, move the mouse cursor over the information icon in the Template Version column.

### Procedure

1. Download the latest Control Manager widget pool and policy templates (for Control Manager 6.0 and later) component.

   A blue notification appears on the top of the Dashboard and Policy Management screens.

2. Click Update Now in the notification box on either of the screens.

3. Click OK when the update completes.

   The screen refreshes and the logon screen appears.

4. Log on to the web console.


   The Policy Template Settings screen appears.

6. Click Update <version number> in the Policy framework row.

7. To add a new policy template, click Enable in the Action column.

   Administrators can then select the new setting templates from the Product list on the Policy Management screen.

8. To update an existing template, click Update <version number> in the Action column.

   To see more information about the update, click Details in the Action column.
Once the update completes, administrators can check the updated features by editing existing policies. Under the Settings section, a red message appears next to the new feature title.
Users in Control Manager

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Control Manager or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

This chapter explains account roles and authentication methods, how to administer Control Manager to manage policies affecting Endpoint Encryption user, and how to control information access by using the specialized Endpoint Encryption Users widget. This chapter also explains how to use PolicyServer MMC to restore deleted Endpoint Encryption users.

Note
For a description of Endpoint Encryption user roles and authentication, see Endpoint Encryption Users on page 2-4.

Topics include:

• Endpoint Encryption Users Widget on page 4-9
• Adding Users to Endpoint Encryption on page 6-4
• Finding a User on page 6-10
• Modifying a User on page 6-10
• *Working with Passwords on page 6-11*

• *Working with Policy Membership on page 6-16*
Endpoint Encryption Users Widget

The Endpoint Encryption Users widget provides user management capability directly from the Control Manager dashboard. Use the Endpoint Encryption Users widget to add or remove Endpoint Encryption user accounts, reset passwords, change permissions, configure policy group priority, import from Active Directory, and search for specific user accounts.

**Note**

For information about managing users with the Endpoint Encryption Users widget, see Users in Control Manager on page 6-1.

For information about adding existing Endpoint Encryption users to a policy, see Configuring Endpoint Encryption Users Rules on page 3-14.

**Figure 6-1. Endpoint Encryption Users Widget**
### Table 6-1. Endpoint Encryption Users Widget Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The total number of users in the entire Enterprise, selected policy, or specified search.</td>
</tr>
<tr>
<td>2</td>
<td>All users in the Enterprise, selected policy, or specified search.</td>
</tr>
<tr>
<td>3</td>
<td>Click the icon to filter which Endpoint Encryption users appear in the table.</td>
</tr>
<tr>
<td>4</td>
<td>Click the Show drop-down box to select the Enterprise or a specific policy to show in the table.</td>
</tr>
<tr>
<td>5</td>
<td>Use the search field to specify parameters to search against.</td>
</tr>
<tr>
<td>6</td>
<td>Click the icon to configure widget settings.</td>
</tr>
<tr>
<td>7</td>
<td>Click the icon to refresh widget data.</td>
</tr>
<tr>
<td>8</td>
<td>Click the icon to view online help.</td>
</tr>
<tr>
<td>9</td>
<td>Click the icon to close the widget.</td>
</tr>
<tr>
<td>10</td>
<td>View the last time that the widget synchronized data with PolicyServer.</td>
</tr>
<tr>
<td>11</td>
<td>Click the icon to view user attributes or to perform actions on any selected user.</td>
</tr>
<tr>
<td>12</td>
<td>Click the icon to add individual users, import users from a CSV file, or import users from Active Directory LDAP.</td>
</tr>
</tbody>
</table>

### Adding Users to Endpoint Encryption

Endpoint Encryption has several options to add users to Endpoint Encryption:

- Add users manually, one at a time
- Bulk import numerous users with a CSV file
- Use the External Directory Browser with Active Directory
Adding a New Enterprise User

Procedure

1. From the Endpoint Encryption Users widget, click the icon and then select Add new user.

   The Add New User screen appears.

2. Specify the new user account details:
   - User name
   - First name
   - Last name
   - Employee ID
   - Email address
   - Freeze
   - User type
   - One policy
   - Authentication method

   Note
   For information about the configuration options, see Add New User Options on page 6-6.

3. Click Add.

The new user is added to the Enterprise. To assign the user to a policy, see Adding an Existing User to a Policy on page 6-21.
Add New User Options

The following table explains the options available when adding a new Endpoint Encryption user.

**TABLE 6-2. Add New User Options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the account user name that the user uses to authenticate.</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the user's last name.</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Specify the user's employee ID (optional).</td>
</tr>
<tr>
<td>Email address</td>
<td>Specify user's email address (optional).</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select <strong>Yes</strong> to temporarily lock the account. A locked account cannot log on to Endpoint Encryption devices.</td>
</tr>
<tr>
<td>User type</td>
<td>Select <strong>User</strong>, <strong>Authenticator</strong>, or <strong>Administrator</strong>.</td>
</tr>
<tr>
<td>One group</td>
<td>Select <strong>Yes</strong> to only allow the user to belong to one policy at a time.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Select the authentication method available to the user.</td>
</tr>
</tbody>
</table>

Importing Users from a CSV File

Format each line in the CSV file as follows:

User ID (required), first name, last name, employee ID, email address

For fields with no data, use a comma as a placeholder.

Example: User ID,„„ employee ID, email address
Procedure

1. From the Endpoint Encryption Users widget, click Add User and then select Import Users from a File.

   The Import Users from a File screen appears.

2. Click Choose File to select the CSV file.

   The Open CSV File window appears.

3. Select the file and then click Open.

4. Click Add.

   The users in the CSV file are imported.

Importing Active Directory Users

PolicyServer maintains a user directory separate from the Active Directory database. This allows PolicyServer absolute security over access to all Endpoint Encryption devices, user rights, and authentication methods.

For information about configuring Active Directory integration, see the Endpoint Encryption Installation and Migration Guide.

Procedure

1. Log on to Control Manager.

2. Go to the Endpoint Encryption Users widget.

3. Click the user icon.

4. Select Import Users from Active Directory
The **Import Users from Active Directory** screen appears.

![Import Users from Active Directory](image)

5. Specify the following parameters for the Active Directory LDAP Server:
   - **Host name**
   - **Port**
   - **User name**
   - **Password**

6. Click **Next**.

7. Wait for the specified Active Directory domain to populate.
The Active Directory tree for the specified domain appears in the left pane.

8. From the left pane, use the navigation tree to select the container from which to add users.

The available users populate in the right pane.

9. Do one of the following:
   • Select individual users, then click **Import Selected Users**.
   • Click **Import Everyone in this Container**.

10. Click **OK** to add the users to the specified location.

A confirmation window appears.

11. Click **OK** to confirm.

An import status message displays.

12. Click **Close** to finish, or repeat the procedure to select more users to import.
Finding a User

For a description of the **Endpoint Encryption Users** widget, see *Endpoint Encryption Users Widget on page 4-9.*

---

**Note**

Adding a user to the Enterprise does not assign any policy target to the new user account.

---

**Procedure**

1. Use the **Show** drop-down list to control whether to show data for the entire Enterprise or only selected policy targets.

2. Click the **icon** to filter which Endpoint Encryption users appear in the table.

3. Specify search criteria and then press the ENTER key.

All users matching the search criteria display.

---

Modifying a User

---

**Procedure**

1. Select the user account.

   See *Finding a User on page 6-10.*

2. Do one of the following:

   • Right-click the user in the table and select the following option: **Modify User**

   • Select the user in the table, click the **icon**, and then select the following option: **Modify User**

   The **Modify User** screen appears.

3. Specify the changes, and then click **Save Changes**.
For information about the configuration options, see *Add New User Options on page 6-6.*

## Working with Passwords

When a user forgets the password or misplaces an endpoint, the user can reset the password using methods defined by policies. The following password reset methods are available:

- Microsoft Windows Active Directory
- Control Manager
- PolicyServer MMC
- Remote Help
- Self Help

All of these options involve setting the policy at the Enterprise or at the group/policy level, if necessary. Use the Support Information policy to provide support-related information to users about password resets.

**Note**

For information about configuring support information in Control Manager, see *Endpoint Encryption Policy Settings on page 5-12.*

For information about configuring support information in PolicyServer MMC, see *Support Information Setup on page 11-29.*

## Changing an Enterprise Administrator/Authenticator Password

**Note**

It is not possible modify multiple users' passwords at the same time.
**Procedure**

1. In the **Show** drop-down list, select **Enterprise**.
2. Select the user account.
   
   See *Finding a User on page 6-10*.

3. Do one of the following:
   
   • Right-click the user in the table and select the following option:

   **Change password**

   • Select the user in the table, click the ⌁ icon, and then select the following option:

   **Change password**

---

**Note**

Use the **User Type** column to find the appropriate account role.

---

The **Change Password** screen appears.

4. Specify the new password settings.

5. Click **Save**.

---

**Resetting a Policy Administrator/Authenticator Password**

Changing the password only affects the user name and password combination for the current policy group. Policy group passwords are unique to other policy group passwords. To change the password for the user account across all policy groups, make sure to change the account password at the Enterprise level.

**Procedure**

1. In the **Show** drop-down list, select the appropriate policy name.
2. Select the user account.
   For information about finding the account, see *Finding a User on page 6-10*.

3. Do one of the following:
   • Right-click the user in the table and select the following option:
     **Change password**
   • Select the user in the table, click the password icon, and then select the following option:
     **Change password**

---

**Note**
Use the *User Type* column to find the appropriate account role.

The **Change Password** screen appears.

4. Specify the new password settings.

5. Click **Save**.

---

**Resetting a Fixed Password**

Changing the password only affects the user name and password combination for the current policy group. Policy group passwords are unique to other policy group passwords. To change the password for the user account across all policy groups, make sure to change the account password at the Enterprise level.

**Procedure**

1. In the **Show** drop-down list, select the appropriate group name.

2. Select the user account.
   For information about finding the account, see *Finding a User on page 6-10*.

3. Do one of the following:
Right-click the user in the table and select the following option:

**Change password**

Select the user in the table, click the ⚒️ icon, and then select the following option:

**Change password**

---

**Note**

Use the **User Type** column to find the appropriate account role.

The **Change Password** screen appears.

4. In the **Authentication method** drop-down list, make sure that **Fixed Password** is selected.
5. Specify the new fixed password.
6. Confirm the new fixed password.
7. Click **Save**.

---

**Changing a User to Domain Authentication**

If configured, users can authenticate using Active Directory credentials. It is not possible to change the Active Directory password.

**Procedure**

1. In the **Show** drop-down list, select the appropriate group name.
2. Select the user account.

   For information about finding the account, see *Finding a User on page 6-10*.

3. Do one of the following:
   - Right-click the user in the table and select the following option:
Change password

- Select the user in the table, click the icon, and then select the following option:

**Change password**

**Note**

Use the **User Type** column to find the appropriate account role.

The **Change Password** screen appears.

4. In the **Authentication method** drop-down list, select **Domain**.

5. Click **Save**.

---

**Changing a User to Fixed Password**

Changing the password only affects the user name and password combination for the current policy group. Policy group passwords are unique to other policy group passwords. To change the password for the user account across all policy groups, make sure to change the account password at the Enterprise level.

**Procedure**

1. In the **Show** drop-down list, select the appropriate group name.

2. Select the user account.

   For information about finding the account, see *Finding a User on page 6-10*.

3. Do one of the following:
   
   - Right-click the user in the table and select the following option:

     **Change password**

   - Select the user in the table, click the icon, and then select the following option:
Change password

Note
Use the User Type column to find the appropriate account role.

The Change Password screen appears.

4. In the Authentication method drop-down list, select Fixed Password.

5. Specify the fixed password.

6. Confirm the fixed password.

7. Click Save.

Working with Policy Membership

This section explains how to add or remove users from a policy group, and how to restore a deleted user.

Groups

To streamline policy management, Control Manager merges the PolicyServer MMC group and policy hierarchy together. PolicyServer maintains the same policy and group configuration no matter which management console you prefer. When you create a new policy target in Control Manager, PolicyServer MMC shows a new group that contains the policy configurations and the users added to that policy.

Important
Control Manager always takes precedence. Any modifications to the group assignment in PolicyServer MMC are automatically overwritten the next time that Control Manager synchronizes with PolicyServer.
**Policy Membership**

The following table explains how to understand Endpoint Encryption user policy membership.

---

**Note**

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

---

**Table 6-3. Policy Membership Descriptions**

<table>
<thead>
<tr>
<th>Header</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1, 2, 3</td>
<td>Shows the order that policies are applied to the Endpoint Encryption user. For more information, see <em>Changing a User's Policy Priority on page 6-20.</em></td>
</tr>
<tr>
<td>Policy Name</td>
<td>GP1</td>
<td>Shows the name of all policies that the user is currently assigned.</td>
</tr>
<tr>
<td>Description</td>
<td>Temporary employees policy.</td>
<td>Shows the description of the policy. To change the policy description, see <em>Editing a Policy on page 5-24.</em></td>
</tr>
<tr>
<td>Allow Install</td>
<td>Yes, No</td>
<td>Shows whether the user can install new Endpoint Encryption devices. For more information, see <em>Allowing a User to Install Devices on page 6-19.</em></td>
</tr>
</tbody>
</table>
Viewing a User's Assigned Policies

Use the **Policy Membership** screen to view Endpoint Encryption user policy assignment. Allowing Endpoint Encryption users to install means that the user account is allowed to add new Endpoint Encryption devices to their assigned policy groups by installing the Endpoint Encryption agent software on any endpoint. Changing the priority affects the policy membership of the new Endpoint Encryption devices when the user installs the Endpoint Encryption agent. The highest priority (1) policy is the default policy.

**Procedure**

1. Select the user account.
   
   For information about finding the account, see *Finding a User on page 6-10.*

2. Do one of the following:
   
   • Right-click the user in the table and select the following option: **List policies**
   
   • Select the user in the table, click the 📊 icon, and then select the following option: **List policies**
The Policy Membership screen appears.

![Policy Membership Screen]

3. Optionally change the policy assignment.
   a. Select the check box next to the appropriate policy.
   b. Click Allow Install.
   c. Click Save.

Allowing a User to Install Devices

This option allows Endpoint Encryption users to add Endpoint Encryption devices to a policy without requiring Policy Administrator/Authenticator permissions in the policy. The default is No.

Procedure

1. Go to the Endpoint Encryption user's policy list.
2. Select the check box next to the policy that the user should be able to install devices.

3. Click Allow Client Install.

Changing a User's Policy Priority

The policy priority defines the order that policies are applied when a user logs on the device. The first policy in the policy list is the default policy for the user. When a user installs a device, the device is always assigned to the user's default policy.

Note

The user must be allowed to install to the default group. For more information, see Allowing a User to Install Devices on page 6-19.

Procedure

1. Go to the user's policy list.

2. Select the check box next to the policy to set as the default policy.

3. Click Move to Top.

Adding a New User to a Policy

Policies can only add existing users. To add a user, first use the Endpoint Encryption Users widget to add a new user and then add that user account to a policy. It is not possible to assign a new user directly to a policy using the Endpoint Encryption Users widget.
Procedure

1. Create the new user with the **Endpoint Encryption Users** widget.
   
   See *Adding a New Enterprise User on page 6-5*.

2. Add the user to a policy.
   
   See *Adding an Existing User to a Policy on page 6-21*.

Adding an Existing User to a Policy

It is not possible to directly assign a new user to a policy using the **Endpoint Encryption Users** widget.

**Note**

For information about the available user options in the policy, see *Configuring Endpoint Encryption Users Rules on page 3-14*.

Administrators can change the information of a policy including the policy name, targets, and settings. Only the policy creator can modify the policy.

Control Manager supports the following changes:

- Modifying a filtered policy
- Adding more targets to a specified policy
- Removing some targets from a specified policy

Procedure

1. Go to **Policies > Policy Management**.
   
   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.
   
   The screen refreshes to display policies created for the selected managed product.
3. Click a policy name in the **Policy** column.
   
   The **Edit Policy** screen appears.

4. In the **Users** section, select **Select specific users**.

5. Click **Select User**.

   The **Add Existing Users to Policy** screen appears.

6. Specify the search criteria and then click **Search**.

   Any users matching the search criteria display in the left pane.

7. To add a user to the policy, select the user in the left pane and then click **Add>>**.

   The user account moves to the right pane.

8. To remove a user from the selection, select the user in the right pane and then click **<<Remove**.

   The user account moves to the left pane.

9. Click **Add**.

10. Click **Deploy**.

    The changes apply immediately.
Users in Control Manager

Note

- After clicking **Deploy**, please wait two minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.

- Control Manager enforces the policy settings on the targets every 24 hours.

Removing Users from a Policy

**WARNING!**

- Before removing the Administrator or Authenticator account, reassign this role to another Endpoint Encryption user. Otherwise, only Enterprise Administrator and Enterprise Authenticator accounts can make changes to the policy.

- Removing Endpoint Encryption users from a policy restricts access to all encrypted Endpoint Encryption devices assigned to that policy. Before removing the users, make sure that they back up and decrypt their data.

It is not possible to remove a user from a policy using the Endpoint Encryption Users widget. For information about the available user options, see *Configuring Endpoint Encryption Users Rules on page 3-14*.

Administrators can change the information of a policy including the policy name, targets, and settings. Only the policy creator can modify the policy.

Control Manager supports the following changes:

- Modifying a filtered policy
- Adding more targets to a specified policy
- Removing some targets from a specified policy

**Procedure**

1. Go to **Policies > Policy Management**.

   The **Policy Management** screen appears.
2. Select the type of product settings from the **Product** list.
   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.
   The **Edit Policy** screen appears.

4. Modify the policy.

5. Select all users to remove from the policy, and then click **Remove User From Policy**.

6. Click **Deploy**.
   The changes apply immediately.

---

**Note**

- After clicking **Deploy**, please wait two minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
- Control Manager enforces the policy settings on the targets every 24 hours.

---

**Removing All Users From a Policy**

**Procedure**

1. Go to **Policies > Policy Management**.
   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.
   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.
   The **Edit Policy** screen appears.
4. Expand the Users section, and then select Select specific users, if not already selected.

5. Select all user accounts, then select Remove User.

   All users have been removed from the policy.

6. Click Deploy.

   The changes apply immediately.

---

**Note**

- After clicking Deploy, please wait two minutes for Control Manager to deploy the policy to the targets. Click Refresh on the Policy Management screen to update the status information in the policy list.

   - Control Manager enforces the policy settings on the targets every 24 hours.

---

**Restoring a Deleted User**

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption user.

---

**Procedure**

1. Log on to PolicyServer MMC.

2. Expand the Recycle Bin.

3. Open Deleted Users.

   The right pane loads all deleted users.

4. Right-click the user account, then select Restore User.

   The user is added back to the Enterprise, but does not belong to any policy groups.
Devices in Control Manager

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

This chapter explains how to administer Control Manager to manage policies affecting Endpoint Encryption devices, and how to ensure data security by using the specialized Endpoint Encryption devices widget. This chapter also explains how to use PolicyServer MMC to restore deleted Endpoint Encryption devices.

Topics include:

- Adding a Device to a Policy on page 7-3
- Removing a Device From a Policy on page 7-6
- Endpoint Encryption Devices Widget on page 4-11
- Finding a Device on page 7-9
- Deleting a Device From the Enterprise on page 7-16
- Getting a Software Token on page 7-9
- Getting a Recovery Key on page 7-10
- Viewing Device Attributes on page 7-11
• Killing a Device on page 7-14
• Locking a Device on page 7-15
• Resetting a Device on page 7-15
• Restoring a Deleted Device on page 7-17
Adding a Device to a Policy

Endpoint Encryption devices are automatically added to the default policy assigned to the user installing the Endpoint Encryption agent on the endpoint. To manually add Endpoint Encryption devices to policies in Control Manager, assign policy targets to that policy. The following procedure explains how to add Endpoint Encryption devices to an existing Control Manager policy. For information about adding a new policy, see *Creating a Policy on page 3-10.*

**Note**

Each Endpoint Encryption device can only belong to a single policy.

**Procedure**

1. Go to **Policies > Policy Management.**
   
   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.
   
   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.
   
   The **Edit Policy** screen appears.

4. Modify the policy.

5. Select one of the following policy target options:

   - **None (Draft Only):** Create a policy with no targets (endpoints)
   - **Filter by Criteria:** Endpoint Encryption does not support filtering by criteria
   - **Specify Target(s):** Specify existing endpoints.

**Note**

For more information about policy targets, see *Specifying Policy Targets on page 3-12*
6. Click **Deploy**.

The changes apply immediately.

---

**Note**

- After clicking **Deploy**, please wait two minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.

- Control Manager enforces the policy settings on the targets every 24 hours.

---

**Specifying Policy Targets**

Use the **Specify Target(s)** screen to assign Endpoint Encryption devices to the policy.

---

**Note**

The **Specify Target(s)** screen is available when creating a new policy. For information about creating a policy, see *Creating a Policy on page 3-10*. 

---
Procedure

1. From the Specify Target(s) screen, click the Browse tab.

2. From the left pane, expand the tree to select the managed folder.

   Example: CM-PI-2K8 > Local Folder > TMEE > TMEE > QA2

3. Select any appropriate Endpoint Encryption devices, or select the top check box to select all Endpoint Encryption devices listed on the current page.

4. Click Add Selected Targets.

---

**Note**

To immediately select all devices in the managed folder, click Add All from Selected Folder.

---

“View Action List” and “View Results” update based on the selection.
Removing a Device From a Policy

Procedure

1. Go to Policies > Policy Management.
   
   The Policy Management screen appears.

2. Select the type of product settings from the Product list.
   
   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the Policy column.
   
   The Edit Policy screen appears.

4. Select Specify Targets.
   
   See Specifying Policy Targets on page 3-12.

   Note
   
   Filtering by criteria is not available for Endpoint Encryption.

5. Click Deploy.
   
   The changes apply immediately.

   Note
   
   • After clicking Deploy, please wait two minutes for Control Manager to deploy the policy to the targets. Click Refresh on the Policy Management screen to update the status information in the policy list.

   • Control Manager enforces the policy settings on the targets every 24 hours.
Endpoint Encryption Devices Widget

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

The **Endpoint Encryption Devices** widget provides Endpoint Encryption device management capability directly from the Control Manager dashboard. Use the **Endpoint Encryption Devices** widget to monitor activity, search for Endpoint Encryption devices, or secure endpoint data by initiating lock or erase commands when an endpoint is lost or stolen.

---

**Note**

For information about managing devices with the **Endpoint Encryption Devices** widget, see *Devices in Control Manager on page 7-1.*

For information about adding Endpoint Encryption devices to a policy, see *Specifying Policy Targets on page 3-12.*

---

![Figure 7-2. Endpoint Encryption Devices Widget](image-url)
### TABLE 7-1. Endpoint Encryption Devices Widget Description

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View the total number of devices in the entire Enterprise, selected policy, or specified search.</td>
</tr>
</tbody>
</table>
| 2    | View all devices in the entire Enterprise, selected group, or specified search.  
  * **Device Name**: The computer name associated with the Endpoint Encryption device.  
  * **Agent**: The installed Endpoint Encryption agent.  
  * **FDE Encryption Status**: If Full Disk Encryption agent is installed, the encryption status. For information, see *Full Disk Encryption Status Widget on page 4-13*.  
  * **Status**: The current status of the Endpoint Encryption device. |
| 3    | Click the 🔍 icon to select the Endpoint Encryption agent and filter the devices shown in the table. |
| 4    | Click the **Show** drop-down box to select the entire Enterprise or a specific policy to show in the table. |
| 5    | Use the search field to specify parameters to search against. Any attributes listed in devices attributes can be searched. |
| 6    | Click the 📺 icon to configure widget settings. |
| 7    | Click the 🔄 icon to refresh widget data. |
| 8    | Click the 📚 icon to view online help. |
| 9    | Click the ✗ icon to close the widget. |
| 10   | View the last time that the widget synchronized data with PolicyServer. |
| 11   | Click the 📈 icon to view device attributes or to perform actions on the selected device. |
Finding a Device

For information about the Endpoint Encryption Devices widget user interface, see Endpoint Encryption Devices Widget on page 4-11.

Procedure

1. Go to the Endpoint Encryption Devices widget.

2. Do any or all of the following:
   - Click the icon to select the Endpoint Encryption agent and filter the devices shown in the table.
   - Click the Show drop-down box to select the entire Enterprise or a specific policy to show in the table.
   - Use the search field to specify parameters to search against. Any attributes listed in devices attributes can be searched.

3. Find the device from the table.

Getting a Software Token

Generating a “software token” creates a unique string that you can use to unlock Endpoint Encryption devices and to remotely help Endpoint Encryption users reset forgotten passwords.

Note

The software token is only available in the full version of Full Disk Encryption, not Encryption Management for Apple FileVault or Encryption Management for Microsoft BitLocker.

For information about remote help assistance, see Remote Help Assistance on page 11-27.
Procedure

1. Find the device.

   See Finding a Device on page 7-9

2. Right-click the device and select Soft Token.

   The Software Token screen appears.

3. Get the 16-digit challenge code from the user, and type it into the Challenge field of the Software Token window.

4. Click Get Response.

   The Response field loads with an 8-character string.

5. Tell the user the 8-character string from the Response field.

The Endpoint Encryption device is unlocked and the Endpoint Encryption user can log on to the device.

Getting a Recovery Key

Generating a “recovery key” allows the user to decrypt a hard disk when the user has forgotten the original password or key. The recovery key is only available to Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker agents because they do not use the other recovery methods available in Full Disk Encryption.

Note

The recovery key is used for encrypted devices and is only available as an option when applicable devices are selected.

Procedure

1. Find the device.
See *Finding a Device on page 7-9*

2. Do one of the following:
   - Right-click the device in the table and select **Recovery key**.
   - Select the device in the table, click the ![icon] icon, and then select **Recovery key**.

   The recovery key appears.

3. Copy the recovery key for use on the locked device.

4. Click **OK**.

---

**Viewing Device Attributes**

Use **Device Attributes** to view a current snapshot of the selected device.

---

**Procedure**

1. Find the device.

   See *Finding a Device on page 7-9*

2. Do one of the following:
   - Right-click the device in the table and select **Attributes**.
   - Select the device in the table, click the ![icon] icon, and then select **Attributes**.

   The **Device Attributes** screen appears.

---

**Endpoint Encryption Device Attributes**

The following table describes the Endpoint Encryption device attributes.
### Table 7-2. Endpoint Encryption Device Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Version</td>
<td>2.0.50727.3620</td>
<td>The version and build number for the installed .NET framework</td>
</tr>
<tr>
<td>Common Framework Build Number</td>
<td>5.0.0.84</td>
<td>The Endpoint Encryption agent uses a common framework for encryption. The build number is used to tell whether the agent is up-to-date</td>
</tr>
<tr>
<td>Disk Model</td>
<td>VMware Virtual IDE</td>
<td>The hard disk mode.</td>
</tr>
<tr>
<td>Disk Name</td>
<td>.\PHYSICALDRIVE0</td>
<td>The name of the hard disk.</td>
</tr>
<tr>
<td>Disk Partitions</td>
<td>1</td>
<td>The number of partitions on the disk with the agent installed.</td>
</tr>
<tr>
<td>Disk Size</td>
<td>10733990400</td>
<td>The total capacity of the hard disk (bytes).</td>
</tr>
<tr>
<td>Domain Name</td>
<td>WORKGROUP</td>
<td>The domain that the endpoint is a member.</td>
</tr>
<tr>
<td>Endpoint ID</td>
<td>85b1e3e2a3c25d882540ef6e4818c3e4</td>
<td>The unique ID of the endpoint used for Control Manager integration.</td>
</tr>
<tr>
<td>&lt;Agent&gt; User</td>
<td>maryjane</td>
<td>The user name for the last logged on use.</td>
</tr>
<tr>
<td>&lt;Agent&gt; Version</td>
<td>5.0.0.260</td>
<td>The version and build number for the agent installation.</td>
</tr>
<tr>
<td>Hostname</td>
<td>TREND-4136D2DB3</td>
<td>The endpoint's host name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.152.219</td>
<td>The endpoint's IP address.</td>
</tr>
<tr>
<td><strong>ATTRIBUTE NAME</strong></td>
<td><strong>EXAMPLE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Locale</td>
<td>English (United States)</td>
<td>The language and region that the endpoint is configure.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>TREND-4136D2DB3</td>
<td>The computer name that the endpoint use.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>VMware, Inc.</td>
<td>The manufacturer of the hard dis.</td>
</tr>
<tr>
<td>Model</td>
<td>VMware Virtual Platform</td>
<td>The model of the hard dis.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows NT 5.1.2600 Service Pack 3</td>
<td>The operating system installed on the same hard disk as the agent.</td>
</tr>
<tr>
<td>Operating System Name</td>
<td>Microsoft Windows XP Professional</td>
<td>The common name of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Operating System Service Pack</td>
<td>Service Pack 3</td>
<td>The service pack number of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Operating System Version</td>
<td>5.1.2600.196608</td>
<td>The version number of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Partition Scheme</td>
<td>Classical MBR</td>
<td>The partition scheme for the hard disk</td>
</tr>
<tr>
<td>Processor</td>
<td>x86 Family 6 Model 30 Stepping 5, Genuine Intel</td>
<td>The processor make and model of the endpoint</td>
</tr>
<tr>
<td>Processor Count</td>
<td>2</td>
<td>The number of processors in the endpoint</td>
</tr>
<tr>
<td>Processor Revision</td>
<td>1e05</td>
<td>The processor revision number</td>
</tr>
</tbody>
</table>
### Killing a Device

Initiating a “kill” command deletes all Endpoint Encryption device data. The deleted data is different depending on the scope of data that the associated Endpoint Encryption agent manages. For example, initiating a “kill” command to a Full Disk Encryption device deletes all data from the endpoint, while initiating a “kill” command to a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent. The “kill” command is issued when the Endpoint Encryption agent communicates with PolicyServer.

---

**WARNING!**

Killing a device cannot be undone. Back up all the data before initiating a kill command.

---

**Procedure**

1. Find the device.
   
   See *Finding a Device on page 7-9*

2. Do one of the following:
   
   • Right-click the device in the table and select **Kill**.
   
   • Select the device in the table, click the icon, and then select **Kill**.

---

<table>
<thead>
<tr>
<th><strong>ATTRIBUTE NAME</strong></th>
<th><strong>EXAMPLE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Taipei Standard Time</td>
<td>The time zone that the endpoint resides</td>
</tr>
<tr>
<td>Total Physical Memory</td>
<td>2047MB</td>
<td>The total RAM installed in or allocated to the endpoint</td>
</tr>
<tr>
<td>Type</td>
<td>X86-based PC</td>
<td>The endpoint processor type</td>
</tr>
<tr>
<td>Windows User Name</td>
<td>TREND-4136D2DB3\admin</td>
<td>The user name of the Windows account that last logged on the endpoint</td>
</tr>
</tbody>
</table>
3. At the warning message, click Yes to confirm.

Locking a Device

Initiating a “lock” command to the Endpoint Encryption device prevents Endpoint Encryption user access until after performing a successful Remote Help authentication. Locking a device reboots the endpoint and forces it into a state that requires Remote Help. The lock command is issued when the Endpoint Encryption agent communicates with PolicyServer.

Procedure

1. Find the device.
   
   See Finding a Device on page 7-9

2. Do one of the following:
   
   • Right-click the device in the table and select Lock.
   
   • Select the device in the table, click the icon, and then select Lock.

3. At the warning message, click Yes to confirm.

Resetting a Device

Initiating a “soft reset” command reboots the endpoint. The command issues the next time that the agent communicates with PolicyServer.

Procedure

1. Find the device.
   
   See Finding a Device on page 7-9

2. Do one of the following:
• Right-click the device in the table and select **Soft Reset**.

• Select the device in the table, click the ![icon](image.png) icon, and then select **Soft Reset**.

3. At the warning message, click **Yes** to confirm.

### Deleting a Device From the Enterprise

Deleting any Endpoint Encryption device from the Enterprise also removes the device from all policy groups. The deleted Endpoint Encryption device continues functioning as long as connectivity and password policies are current on the device. However, Endpoint Encryption users cannot recover files if the Endpoint Encryption device has a critical hardware failure after it has been removed from the Enterprise. To mitigate this risk, immediately decrypt the Endpoint Encryption device and uninstall the Endpoint Encryption agent software.

For information about removing a device from a specific policy, but not the Enterprise, see *Removing a Device From a Policy on page 7-6.*

---

**WARNING!**

Make sure to decrypt the device (files or hard disk) and uninstall the Endpoint Encryption agent before deleting a device from the Enterprise. Failure to do so may result in data loss.

---

**Procedure**

1. Uninstall the Endpoint Encryption agent from the endpoint.

   ---

   **Note**

   For information about uninstalling Endpoint Encryption agents, see the *Endpoint Encryption Installation and Migration Guide.*

   ---

2. Find the device.

   See *Finding a Device on page 7-9*

3. Do one of the following:
• Right-click the device in the table and select **Delete Device**.

• Select the device in the table, click the icon, and then select **Delete Device**.

4. At the warning message, click **Yes** to confirm.

The Endpoint Encryption device is deleted from the Enterprise.

---

**Note**

For information about adding the Endpoint Encryption device back the Enterprise, see *Restoring a Deleted Device on page 7-17*.

---

**Restoring a Deleted Device**

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption device.

---

**Procedure**

1. Log on to PolicyServer MMC.

2. Expand the Enterprise, then go to **Enterprise Maintenance**.

3. Expand the **Recycle Bin**.

4. Open **Deleted Devices**.

   The right pane loads all deleted Endpoint Encryption devices.

5. Right-click the Endpoint Encryption device and select **Restore Device**.

   The Endpoint Encryption device is added back to the Enterprise, but does not belong to any policy groups.
Part III
Administration with Endpoint Encryption Policy Server MMC
Getting Started with PolicyServer MMC

Before configuring PolicyServer MMC to manage PolicyServer, make sure to install and configure PolicyServer services and databases.

Note
For information about installing and configuring PolicyServer MMC, see the Endpoint Encryption Installation and Migration Guide available at:


Topics include:

• About PolicyServer MMC on page 8-2
• Logging on to PolicyServer MMC on page 8-2
• PolicyServer MMC Interface on page 8-4
• Working with Groups and Users on page 8-5
• Understanding Policy Controls on page 8-15
• Disabling Agents on page 8-19
About PolicyServer MMC

The PolicyServer Microsoft Management Console plug-in (PolicyServer MMC) is the native management console for Endpoint Encryption policy, user, and device administration.

Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

Use PolicyServer MMC to centrally manage:

- All Endpoint Encryption users, devices, and groups
- All policies including encryption, password complexity and authentication
- Remote device actions, including killing a device, erasing data, or delaying authentication
- Event logs about authentication events, management events, device encryption status, and security violations
- Remote Help password reset process
- Auditing and reporting options

Logging on to PolicyServer MMC

Configure the Enterprise name and the Enterprise Administrator account during PolicyServer installation. For information about the free 30-day Trial License, see Trial License on page 17-3.

Procedure

1. To open PolicyServer MMC, do one of the following:
   - Double-click the PolicyServer MMC shortcut on the desktop
   - Go to the folder specified during installation, then double-click PolicyServerMMC.exe
The PolicyServer MMC authentication screen appears.

![PolicyServer Login](image)

**FIGURE 8-1. The PolicyServer MMC Authentication Screen**

2. Specify the following parameters:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Specify the Enterprise.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the user name of an Enterprise Administrator account.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password for the user name.</td>
</tr>
<tr>
<td>Server</td>
<td>Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.</td>
</tr>
</tbody>
</table>

3. Optional: To use a smart card to authenticate, select **Use Smart Card**.

4. Click **Login**.

5. Wait for PolicyServer MMC to connect to PolicyServer.
The PolicyServer MMC opens.

**PolicyServer MMC Interface**

The PolicyServer MMC interface contains the following panes:

![Image of PolicyServer MMC Interface]

**Figure 8-2. PolicyServer MMC Interface**

**Table 8-1. PolicyServer MMC Interface Description**

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left (1)</td>
<td>Use the left pane to view users, groups, policies, devices, and agents. Expand a node to manage nested items within the tree structure. Opening an item updates the content in the right pane.</td>
</tr>
<tr>
<td>Right (2)</td>
<td>Use the right pane to modify policies, update user and group information, view reports, and maintain other functions. The exact format of the information shown in the right pane depend from the left pane.</td>
</tr>
</tbody>
</table>

Within the left pane tree structure, there are a number of different nodes. The following table describes each node:
<table>
<thead>
<tr>
<th><strong>NODE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Users</td>
<td>View all administrator and user accounts within the Enterprise. To see group affiliation, open the group and then click <strong>Users</strong>.</td>
</tr>
<tr>
<td>Enterprise Devices</td>
<td>View all instances of Endpoint Encryption agents and which Endpoint Encryption device they are connecting from. To see group affiliation, open the group and then click <strong>Devices</strong>.</td>
</tr>
<tr>
<td>Enterprise Policies</td>
<td>Control whether agents can connect to PolicyServer. Also, manage all enterprise policies. Group policies override enterprise policies.</td>
</tr>
<tr>
<td>Enterprise Log Events</td>
<td>View all log entries for the enterprise.</td>
</tr>
<tr>
<td>Enterprise Reports</td>
<td>Manage various reports and alerts. No group-only reports are available.</td>
</tr>
<tr>
<td>Enterprise Maintenance</td>
<td>Manage the PolicyServer MMC application plug-ins.</td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>View deleted Endpoint Encryption users and devices.</td>
</tr>
<tr>
<td>Groups</td>
<td>Manage Endpoint Encryption users, devices, policies and log events for a collection of users.</td>
</tr>
</tbody>
</table>

## Working with Groups and Users

This section explains how to get started with the PolicyServer MMC groups and users. First define the users and groups, and then assign users to groups. It is also possible to add new users directly to a group. At least one Top Group is required.

User and group recommendations:

- Follow the Active Directory structure.

- Create a new group whenever there is a policy difference between groups of users. If one group requires domain authentication and another requires fixed password, then two separate groups are required.
• Create multiple groups to minimize access. All members of a group are allowed access to any Endpoint Encryption device in that group.

Defining Users and Groups

Define all roles and group affiliations before adding any users or groups.

1. Identify Enterprise Administrator/Authenticator accounts.
2. Create Enterprise Administrator/Authenticator accounts.
3. Identify groups.
4. Create groups.
5. Identify Group Administrator/Authenticator accounts.
6. Create Group Administrator/Authenticator accounts.
7. Identify users to be assigned to each group.
8. Import or create new users each group.

Adding a Top Group

Groups simplify managing Endpoint Encryption agents, users, policies, subgroups, and devices. A Top Group is the highest level group.

Note

It is not possible to add the Enterprise Administrator or Enterprise Authenticator accounts to groups. To create a Group Administrator, add a user and change the account permissions within the group. For more information, see Modifying a User on page 11-9.

Procedure

1. Right-click the Enterprise in the left pane, then click Add Top Group.
The Add New Group screen appears.

2. Specify the name and description for the group.

3. If using Endpoint Encryption devices that do not support Unicode, select Support Legacy Devices.

---

**Note**

Some legacy devices may not be able to communicate with PolicyServer using Unicode. Assign Unicode and legacy Endpoint Encryption devices to different groups.

---

4. Click Apply.
5. At the confirmation message, click **OK**.
   The new group is added to the tree structure in the left pane.

---

**Adding a New User to a Group**

---

**Note**

Adding a user to the Enterprise does not assign the user to any groups

Adding a user to a group adds the user to the group and to the Enterprise

---

**Procedure**

1. Expand the group and open **Users**.
2. Go to the right pane and right-click the whitespace, then select **Add New User**.
   The **Add New User** screen appears.
3. Specify the following options:

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the user name for the new user account (required).</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the first name for the new user account (required).</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the last name for the new user account (required).</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>Specify the employee ID for the new user account (optional).</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log devices.</td>
</tr>
<tr>
<td>Group User Type</td>
<td>Select the privileges of the new account.</td>
</tr>
</tbody>
</table>

**Note**
For information about account roles, see *Endpoint Encryption User Roles on page 2-5.*
<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Options include:</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• Authenticator</td>
</tr>
<tr>
<td></td>
<td>• Administrator</td>
</tr>
<tr>
<td>Note</td>
<td>It is not possible to add Enterprise Administrator or Enterprise Authenticator accounts to groups.</td>
</tr>
<tr>
<td>One Group</td>
<td>Select whether the new user account is allowed to be a member of multiple group policies.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the method that the new user account uses to log on to Endpoint Encryption devices.</td>
</tr>
<tr>
<td>method</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The default authentication method for users is None.</td>
</tr>
</tbody>
</table>

For information about account roles, see *Devices and Users Overview on page 2-1.*

4. **Click OK.**

The new user is added to the selected group and to the Enterprise. The user can now log on to Endpoint Encryption devices.

---

**Adding a New Enterprise User**

The following procedure explains how to add new Endpoint Encryption users to the Enterprise.
**Note**
Adding a new Endpoint Encryption user to the Enterprise does not assign the user to any groups.

Adding a new Endpoint Encryption user to a group adds the user to the group and to the Enterprise.

**Procedure**

1. To access Enterprise Users, do one of the following:
   - Expand the Enterprise, then open *Enterprise Users*.
   - Expand the Enterprise, expand the group, then open *Users*.

2. Right-click the white space in the right pane and select *Add User*.

   The *Add New User* screen displays.

![Add New User](image)

**Figure 8-6. Add New User screen**

3. Specify the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the user name for the new user account (required).</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the first name for the new user account (required).</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the last name for the new user account (required).</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>Specify the employee ID for the new user account (optional).</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on to devices.</td>
</tr>
<tr>
<td>Group User Type</td>
<td>Select the privileges of the new account. For information about account roles, see Devices and Users Overview on page 2-1.</td>
</tr>
<tr>
<td></td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• Authenticator</td>
</tr>
<tr>
<td></td>
<td>• Administrator</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>It is not possible to add Enterprise Administrator or Authenticator accounts to groups.</td>
</tr>
<tr>
<td>One Group</td>
<td>Select whether the new user account is allowed to be a member of multiple group policies.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Select the method that the new user account uses to log on to Endpoint Encryption devices. For information about authentication methods, see Devices and Users Overview on page 2-1.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>The default authentication method for users is None.</td>
</tr>
</tbody>
</table>
The new Endpoint Encryption user is added the Enterprise. The user cannot log on to Endpoint Encryption devices until the user account is added to a group.

Adding an Existing User to a Group

A user can be a member of multiple groups.

Procedure

1. Expand the group in the left pane, then click Users.
2. Go to the right pane and right-click the whitespace, then select Add Existing User.
The **Add Users To Group** screen appears.

![Add Users To Group Screen](image)

**FIGURE 8-7. Add Users To Group Screen**

3. Specify user details and then click **Search**.
   
The **Source** field populates with any accounts that match the search criteria.

4. Select users from the **Source** list and click the blue arrow to add them.
   
   For information about search icons, see *Add/Remove Search Result Icons on page 11-15*.
   
The selected user moves to the **Destination** list.

5. To change a user password:
   
   a. In the **Destination** list, highlight the user.
   
   b. Click **Enter User Password** located at the bottom of the window.
c. In the window that appears, specify the user’s authentication method.

d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

   The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

---

**Understanding Policy Controls**

After adding and configuring the users and groups, set policies for the Enterprise or group. Each group (whether a Top Group or a subgroup) contains a “Policies” node with policies specific to each agent and other common policies that affect all agents and authentication.

---

**Note**

To disable or enable policies at the Enterprise or group level, see *Accessing Policies on page 9-4*.

For information about the PolicyServer MMC interface, see *PolicyServer MMC Interface on page 8-4*.

---

**Policy Visual Indicators**

The small circles to the left of each policy indicate one of the following states:

- Policy level
- Group modification status
- Single or multiple array of values
- Whether the policy contains sub-policies
**Table 8-3. Policy Indicators**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Single yellow circle" /></td>
<td>A single yellow circle indicates the policy value is inherited from the parent group or the Enterprise.</td>
</tr>
<tr>
<td><img src="image" alt="Single blue circle" /></td>
<td>A single blue circle indicates a policy has been modified for the group.</td>
</tr>
<tr>
<td><img src="image" alt="Three blue circles" /></td>
<td>Three blue circles indicate the policy may have multiple arrays of values.</td>
</tr>
<tr>
<td><img src="image" alt="Three multi-colored circles" /></td>
<td>Three multi-colored (red, blue, green) circles indicate the policy will always have one or more sub-policies.</td>
</tr>
</tbody>
</table>

**Policy Fields and Buttons**

The following table explains the fields and buttons to control policies in PolicyServer MMC. All modified values are propagated to a group's subgroups. Only the relevant fields and buttons show in a selected policy.

**Table 8-4. Policy Fields and Buttons**

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
<th>Changeable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Saves changes to the selected policy</td>
<td>N/A</td>
</tr>
<tr>
<td>Description</td>
<td>Explains the selected policy</td>
<td>No</td>
</tr>
<tr>
<td>Policy Range</td>
<td>Displays the value range that the selected policy can fall between</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy Value</td>
<td>Depending on the policy, displays the actual value of the selected policy, whether it contains a string, number, or series of entries</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy Multiple Value</td>
<td>Specifies whether this policy can be used multiple times for different settings (multiple “if found” strings)</td>
<td>No</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Displays the name of the selected policy</td>
<td>No</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Specifies the category for the selected policy</td>
<td>No</td>
</tr>
</tbody>
</table>
## Field/Button Description

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
<th>Changeable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise controlled</td>
<td>Makes this policy mirror changes to the same policy at the Enterprise level</td>
<td>Yes</td>
</tr>
<tr>
<td>Save to subgroups</td>
<td>Pushes policy settings to the same policy in all subgroups</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Modifying Policies

The PolicyServer MMC has a common set of windows to modify policies. Different types of input are available depending on what the policy controls and which parameters are required. This task gives a general overview about editing a policy. The steps required to edit one policy are different to modify another policy.

**Note**

For more information about modifying policies, including explanations about configuring different policy types, see *Accessing Policies on page 9-4*.

### Procedure

1. Expand the **Enterprise**.
2. Select the policy level to modify.
   - For enterprise policies, expand **Enterprise Policies**.
   - For group policies, expand the **Group Name** and then expand **Policies**.
3. Open the specific application or select **Common**.
The policy list displays in the results windows.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Policy Value</th>
<th>Policy Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolicyServer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Console</td>
<td>3 items</td>
<td></td>
</tr>
<tr>
<td>Console Timeout</td>
<td>20</td>
<td>1 - 60</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>0</td>
<td>0 - 100</td>
</tr>
<tr>
<td>Legal Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>10 items</td>
<td></td>
</tr>
<tr>
<td>Authenticator</td>
<td>9 items</td>
<td></td>
</tr>
<tr>
<td>Log Alerts</td>
<td>2 items</td>
<td></td>
</tr>
<tr>
<td>PDA</td>
<td>7 items</td>
<td></td>
</tr>
<tr>
<td>Service Pack Download</td>
<td>2 items</td>
<td></td>
</tr>
<tr>
<td>Welcome Message</td>
<td>4 items</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8-8. Modifying a Policy**

4. Go to a policy and double-click to open the editor window.
For example, the “Console Timeout” policy:

![Console Timeout Policy Editor Window](image)

**Figure 8-9. “Console Timeout” Policy Editor Window**

5. Specify changes appropriate for the policy, then click **OK**.

---

**Disabling Agents**

All Endpoint Encryption agents are enabled by default.

**Procedure**

1. Log on to PolicyServer MMC.
See *Logging on to PolicyServer MMC on page 8-2*. 

2. Do one of the following:
   - To disable the agent across the Enterprise, click **Enterprise Policies**.
   - To disable the agent for users in the group only, expand the group and then click **Policies**.

   All applications appear in the right pane.

3. Right-click the application and then select **Disable**.

**Figure 8-10. Enable/Disable Agents**

The Endpoint Encryption agent is disabled. Endpoint Encryption users cannot log on devices using this agent.
Policies in PolicyServer MMC

This chapter explains how to manage and configure Endpoint Encryption policies with PolicyServer MMC.

**Note**
For information about the policy mapping between PolicyServer MMC and Control Manager, see *Policy Mapping Between Management Consoles on page D-1*.

Topics include:

- **Policy Overview on page 9-2**
- **Policy Mapping Between Management Consoles on page D-1**
- **Automatic Policy Synchronization on page 9-14**
- **PolicyServer Policies on page 9-14**
- **Configuring Full Disk Encryption Rules on page 3-15**
- **Configuring File Encryption Rules on page 3-17**
- **Common Policies on page 9-30**
Policy Overview

This section explains how to use various windows to change a policy, but does not explain the process to modify every policy. PolicyServer MMC has a common set of windows to use when modifying a policy. One policy may have an editor window available to edit the numbers, ranges and values associated with the policy while another policy may have a window to modify text strings.

When managing policies, note the following:

- Policies are configurable by the agent within each group.
- Policy inheritance only occurs when a subgroup exists. For information about group permissions, see About Groups on page 10-2.
- Every policy has a default value.

Policy Visual Indicators

The small circles to the left of each policy indicate one of the following states:

- Policy level
- Group modification status
- Single or multiple array of values
- Whether the multiple policy contains sub-policies

<table>
<thead>
<tr>
<th>Table 9-1. Policy Indicators</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Yellow Circle]</td>
<td>A single yellow circle indicates the policy value is inherited from the parent group or the Enterprise.</td>
</tr>
<tr>
<td>![Blue Circle]</td>
<td>A single blue circle indicates a policy has been modified for the group.</td>
</tr>
<tr>
<td>![Three Blue Circles]</td>
<td>Three blue circles indicate the policy may have multiple arrays of values.</td>
</tr>
</tbody>
</table>
Three multi-colored (red, blue, green) circles indicate the policy will always have one or more sub-policies.

Policy Fields and Buttons

The following table explains the fields and buttons to control policies in PolicyServer MMC. All modified values are propagated to a group's subgroups. Only the relevant fields and buttons show in a selected policy.

**Table 9-2. Policy Fields and Buttons**

<table>
<thead>
<tr>
<th>FIELD/BUTTON</th>
<th>DESCRIPTION</th>
<th>CHANGEABLE?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Saves changes to the selected policy</td>
<td>N/A</td>
</tr>
<tr>
<td>Description</td>
<td>Explains the selected policy</td>
<td>No</td>
</tr>
<tr>
<td>Policy Range</td>
<td>Displays the value range that the selected policy can fall between</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy Value</td>
<td>Depending on the policy, displays the actual value of the selected policy, whether it contains a string, number, or series of entries</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy Multiple Value</td>
<td>Specifies whether this policy can be used multiple times for different settings (multiple “if found” strings)</td>
<td>No</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Displays the name of the selected policy</td>
<td>No</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Specifies the category for the selected policy</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise controlled</td>
<td>Makes this policy mirror changes to the same policy at the Enterprise level</td>
<td>Yes</td>
</tr>
<tr>
<td>Save to subgroups</td>
<td>Pushes policy settings to the same policy in all subgroups</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Accessing Policies

Every group in PolicyServer MMC contains one or more policy folders. The right pane shows the results window, which provides controls to:

- Display a list of policies and their values
- Modify a policy using the editor window
- Run reports and other log events
- Run enterprise maintenance

Note
For information about the PolicyServer MMC interface, see PolicyServer MMC Interface on page 8-4.

Selecting a Policy for Modification

Procedure

1. Go to Group Name > Policies and select the appropriate node.
   Example: Group1 > Policies > Full Disk Encryption.

2. Go to the specific policy.
   Example: Common > Client > Allow User to Uninstall.

3. Right-click the policy and select Properties.

Editing Policies with Ranges

Some policies have controls to set a range of policy values, such as the minimum and maximum length for a password.
An example of editing policies with ranges is the **Failed Login Attempts Allowed** policy. **Failed Login Attempts Allowed** controls whether a device locks when a user exceeds the number of failed authentication attempts allowed.

**Figure 9-1. Policy with Ranges Window**

Using the parameters defined in the **Policy Range** fields, indicate the number of failed authentication attempts allowed per user in the **Policy Value** field.

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.

2. In the **Minimum** field, specify the lowest number of unsuccessful authentication attempts allowed by a user in this group before locking the device.
Note

The minimum and maximum values for the policy range can be the same as the parent's range, or they can be modified with unique values. It is not possible to extend the minimum and maximum values.

3. In the **Maximum** field, specify the highest number of authentication attempts that can be made by a user in this group before authentication fails and the device is locked.

4. In the **Policy Value** field, specify the number of failed authentication attempts allowed for a user in this group before the device is locked.

5. Click **OK** to save changes.

The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

---

**Editing Policies with True/False or Yes/No Responses**

Some policies only have True/False or Yes/No options. For this example, **Preboot Bypass** is used.

A Group Administrator can define whether the Full Disk Encryption preboot appears before Windows starts. If the parent group allows **Yes** and **No**, then the subgroup Group Authenticators have the right to set the range to **Yes** and **No**, just **Yes**, or just
No. If the parent group has set the range to either Yes or No, then the subgroup Group Administrator can only select that same range.

![Edit Policy Value](image)

**Figure 9-2. Policy with Yes/No Values**

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. Specify policy options.
   - The **Policy Value** field sets whether the policy is turned on.
   - The **Range** field sets whether the policy is available to other users or groups.

   Example: if the policy is set to No, then the policy will not be available to set to Yes.
Note
Removing an option from Policy Range removes the value from the Policy Value drop-down in the current group and all subgroups.

3. Click OK to save changes.

The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

Editing Policies with Multiple-choice / Single-selection

Some policies have multiple options available for selection. The Device Locked Action policy is edited in a multiple-choice/single-selection window. You can only select one
Policy Value. In this example, the Group Administrator must define the action to take when a user exceeds the allowed number of authentication attempts.

Figure 9-3. Policy with Multiple Choice/Single Selection

Procedure

1. Right-click the policy to be modified and then click Properties.
2. Select a default setting from the Policy Value drop-down list.
3. Select the available options for the Policy Range area.
4. Click **OK** to save changes.

The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.
Editing Policies with Text String Arguments

Some policies have an editable text string for single array arguments. The **Dead Man Switch** policy is an example of a policy that provides the capability to specify a string of text.

![Figure 9-4. Policy with Text String Argument](image)

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. Specify the sequence of characters for this policy in the **Policy Value** field.

3. Click **OK** to save changes.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

---

**Editing Policies with Multiple Options**

Some policies have multiple options stored in subpolicies affecting that policy. Multiple option policies create separate lines in a text string, and each new line in the string is a subpolicy. For example, the **IF Found** policy displays how to return a found device. A normal address format displays the name, street address, and city/state/zip on three separate lines.

---

**Note**

Depending on the policy, multiple options is generally limited to six subpolicies.

---

**Procedure**

1. Right-click the policy to modify and then click **Add**.
2. Specify details in the **Policy Value** field.

**Note**
Depending on the policy, you may need to modify the added policy by right-clicking and selecting **Properties**.

3. Click **OK** to save changes.

**Figure 9-6. If Found Policy: Results After Adding Multiple Options**

4. If needed, add a new option.

5. To make changes, right-click the child policy, then select **Properties**.

The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.
Automatic Policy Synchronization

The following list explains the events that initiate policy synchronization between all Endpoint Encryption agents and PolicyServer.

• After the operating system loads and the Endpoint Encryption agent service starts

Note
For information about Endpoint Encryption services, see Endpoint Encryption Services on page C-1.

• When the Full Disk Encryption preboot starts (Full Disk Encryption only)
• The time duration of the Sync Interval policy elapses

Open the About screen in the Endpoint Encryption agent to manually synchronize policies.

Note
Endpoint Encryption device actions initiate after the Endpoint Encryption agent receives policy updates.

PolicyServer Policies

This section explains the configurable options for policies affecting PolicyServer.

Admin Console Policies

The following table explains the policies governing PolicyServer MMC.
TABLE 9-3. PolicyServer Admin Console Policy Descriptions

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Timeout</td>
<td>Exit the administration tool after the Timeout (minutes) has expired with no activity.</td>
<td>1-60</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 20</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>Lockout the administrator logon after this number of consecutive failed log on attempts.</td>
<td>0-100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Legal Notice</td>
<td>Contains the legal notice that must be displayed before the Administrator or Authenticator can use the administration tools.</td>
<td>1-1024 chars</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
</tbody>
</table>

Administrator Policies

The following table explains policies governing PolicyServer Group Administrator privileges.

TABLE 9-4. PolicyServer Administrator Policy Descriptions

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Devices</td>
<td>Specify whether the Group Administrator is allowed to add devices.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Add Users</td>
<td>Specify whether the Group Administrator is allowed to add new users.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Add Users to Enterprise</td>
<td>Specify whether the Group Administrator is allowed to add new users to the enterprise.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Add/Modify Groups</td>
<td>Specify whether the Group Administrator is allowed to add/modify subgroups.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
</tbody>
</table>
### Authenticator Policies

The following table explains policies governing Enterprise and Group Authenticator rights and privileges.

**TABLE 9-5. PolicyServer Administrator Policy Descriptions**

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Devices</td>
<td>Specify whether Enterprise and Group Authenticators are allowed to add devices.</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Add Users</td>
<td>Specify whether Enterprise and Group Authenticators are allowed to add new users.</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Description</td>
<td>Value Range and Default</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
</tbody>
</table>
| Add Users to Enterprise         | Specify whether Enterprise and Group Authenticators are allowed to add new users to the enterprise. | Yes, No                
|                                 |                                                                             | Default: No             |
| Add/Modify Groups               | Specify whether Enterprise and Group Authenticators are allowed to add/modify subgroups. | Yes, No                
|                                 |                                                                             | Default: No             |
| Copy/Paste Groups               | Specify whether Enterprise and Group Authenticators are allowed to copy and paste subgroups. | Yes, No                
|                                 |                                                                             | Default: No             |
| Remove Devices                  | Specify whether Enterprise and Group Authenticators are allowed to remove devices. | Yes, No                
|                                 |                                                                             | Default: No             |
| Remove Groups                   | Specify whether Enterprise and Group Authenticators are allowed to remove subgroups. | Yes, No                
|                                 |                                                                             | Default: No             |
| Remove Users                    | Specify whether Enterprise and Group Authenticators are allowed to remove users. | Yes, No                
|                                 |                                                                             | Default: No             |
| Remove Users from Enterprise    | Specify whether Authenticators are allowed to remove users from the enterprise. | Yes, No                
|                                 |                                                                             | Default: No             |

Log Alert Policies

The following table explains policies governing email messages sent for important PolicyServer log events.
<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Email Address</td>
<td>Specify the email address that is used as the source email address for the alerts email message.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>SMTP Server Name</td>
<td>Specify the SMTP server responsible for sending alert email messages.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
</tbody>
</table>

**Service Pack Download Policies**

The following table explains policies governing when agents automatically download service packs.

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Pack Download Begin Hour</td>
<td>Set the time to download service packs.</td>
<td>0-23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Service Pack Download End Hour</td>
<td>Set the time to stop downloading any service pack.</td>
<td>0-23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
</tbody>
</table>

**Welcome Message Policies**

The following table explains policies governing whether to send a welcome message to users when they have been added to a group.
**TABLE 9-8. PolicyServer Welcome Message Policy Descriptions**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
<th>Value Range and Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Contains the welcome message file.</td>
<td>1-1024 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>SMTP Server Name</td>
<td>Specify the SMTP server responsible for sending welcome email messages.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Source Email</td>
<td>Specify the email address that is used as the source email address for welcome email message.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Subject</td>
<td>The Welcome message subject line.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
</tbody>
</table>

**Full Disk Encryption Policies**

This section explains the configurable options for policies affecting the following Full Disk Encryption agents:

- Full Disk Encryption
- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

**Client Policies**

The following table explains the policies affecting access to the Full Disk Encryption Recover Console and un installing the agent.
Note

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

TABLE 9-9. Full Disk Encryption Client Policy Descriptions

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow User Recovery</td>
<td>Specify if users are allowed to access system recovery utilities on the device.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Allow User to Uninstall</td>
<td>Specify whether user can uninstall Full Disk Encryption.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
</tbody>
</table>

Encryption Policies

The following table explains the Full Disk Encryption encryption policy. The encrypt device policy affects the Full Disk Encryption, Encryption Management for Apple FileVault, and Encryption Management for Microsoft BitLocker agents.

TABLE 9-10. Full Disk Encryption Encryption Policy Descriptions

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Device</td>
<td>Specify whether to encrypt the device.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
</tbody>
</table>

Login Policies

The following table explains the policies that govern logging on to the Full Disk Encryption agent.
Note

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

### Table 9-11. Full Disk Encryption Login Policy Descriptions

<table>
<thead>
<tr>
<th><strong>Policy Name</strong></th>
<th><strong>Description</strong></th>
<th><strong>Value Range and Default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Action</td>
<td>Specify the action to be taken when the device has failed to communicate with the PolicyServer as specified in the policy Account Lockout Period.</td>
<td>Erase, Remote Authentication</td>
</tr>
<tr>
<td></td>
<td>• Erase: All content on the device is wiped.</td>
<td>Default: Remote Authentication</td>
</tr>
<tr>
<td></td>
<td>• Remote Authentication: Require user to perform remote authentication.</td>
<td></td>
</tr>
<tr>
<td>Account Lockout Period</td>
<td>Specify the number of days that the client may be out of communication with the PolicyServer.</td>
<td>0-999</td>
</tr>
<tr>
<td></td>
<td>Default: 360</td>
<td></td>
</tr>
<tr>
<td>Dead Man Switch</td>
<td>Specify a sequence of characters, when entered will erase all contents on the device.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
<td></td>
</tr>
<tr>
<td>Policy Name</td>
<td>Description</td>
<td>Value Range and Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Locked Action</td>
<td>Specify the action to be taken when the device locks.</td>
<td>Time Delay, Erase, Remote Authentication</td>
</tr>
<tr>
<td></td>
<td>• Time Delay: The amount of time that must elapse before the user can</td>
<td>Default: Time Delay</td>
</tr>
<tr>
<td></td>
<td>retry logging on.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Erase: All content on the device is wiped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote Authentication: Require user to perform remote authentication.</td>
<td></td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>Specify the number of failed Login attempts before using Lock Device Time</td>
<td>0-100</td>
</tr>
<tr>
<td></td>
<td>Delay.</td>
<td>Default: 5</td>
</tr>
<tr>
<td>If Found</td>
<td>Specify information to be displayed.</td>
<td>1-255 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Legal Notice</td>
<td>Specify whether a legal notice should be displayed.</td>
<td>Enable/Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Disabled</td>
</tr>
<tr>
<td>Legal Notice Display Time</td>
<td>Specify when the configured legal notice should be displayed to the user.</td>
<td>Installation, Startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Startup</td>
</tr>
<tr>
<td>Legal Notice Text</td>
<td>Specify the body of the legal notice.</td>
<td>Insert File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Lock Device Time Display</td>
<td>Lock device for X minutes if user exceeds Failed Attempts Allowed.</td>
<td>1-999,999 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1</td>
</tr>
<tr>
<td>Preboot Bypass</td>
<td>Specify if the preboot should be bypassed.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Support Info</td>
<td>Display Help Desk information or Administrator contact.</td>
<td>Default: N/A</td>
</tr>
<tr>
<td><strong>Policy Name</strong></td>
<td><strong>Description</strong></td>
<td><strong>Value Range and Default</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Token Authentication</strong></td>
<td>Policy related to physical tokens including smart cards and USB tokens. All sub-policies are visible only when Token Authentication is enabled.</td>
<td>Enable, Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Disable</td>
</tr>
<tr>
<td><strong>OCSP Validation</strong></td>
<td>Verifying certificates via OCSP allows for the revocation of invalid certificates via the CA.</td>
<td>Enable, Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Disable</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All sub-policies are visible only when OCSP Validation is Enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>OCSP CA Certificates</strong></td>
<td>Certificate Authority certificates.</td>
<td>0-1024 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Validation.</td>
<td></td>
</tr>
<tr>
<td><strong>OCSP Expired Certificate Status Action</strong></td>
<td>Defines the action to take if the OCSP certificate status is expired.</td>
<td>Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Denial of Login</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Validation.</td>
<td></td>
</tr>
<tr>
<td><strong>OCSP Grace</strong></td>
<td>A grace period in days that allows authentication to occur even if the OCSP server has not verified the certificate in this number of days.</td>
<td>0-365</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 7</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Validation.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy Name</strong></td>
<td><strong>Description</strong></td>
<td><strong>Value Range and Default</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>OCSP Responders</td>
<td>Certificate Authority certificates.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Default: Yes</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Validation.</td>
<td></td>
</tr>
<tr>
<td>OCSP Responder Certificate</td>
<td>Certificate Authority Certificate</td>
<td>0-1024 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Default: N/A</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Responders.</td>
<td></td>
</tr>
<tr>
<td>OCSP Responder URL</td>
<td>Certificate Authority certificates.</td>
<td>0-1024 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Default: N/A</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Responders.</td>
<td></td>
</tr>
<tr>
<td>OCSP Revoked Certificate Status Action</td>
<td>Defines the action to take if the OCSP certificate status is revoked.</td>
<td>Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Default: Denial of Login</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Responders.</td>
<td></td>
</tr>
<tr>
<td>OCSP Show Success</td>
<td>Whether success of OCSP reply should be displayed.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Default: Yes</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of OCSP Responders.</td>
<td></td>
</tr>
</tbody>
</table>
Policies in PolicyServer MMC

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP Unknown Certificate Status Action</td>
<td>Specify the action when an OCSP certificate status is unknown.</td>
<td>Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access</td>
</tr>
<tr>
<td></td>
<td>This is sub-policy of OCSP Responders.</td>
<td>Default: Denial of Login</td>
</tr>
<tr>
<td>Token Passthru</td>
<td>Pass the token to the desktop GINA for further processing during the boot process.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td>This is sub-policy of OCSP Responders.</td>
<td>Default: No</td>
</tr>
</tbody>
</table>

Password Policies

The following table explains Full Disk Encryption password policies.

**Note**

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**TABLE 9-12. Full Disk Encryption Password Policy Descriptions**

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Methods Allowed</td>
<td>Specify the allowed type(s) of authentication methods that can be used.</td>
<td>Fixed, ColorCode, Pin, Remote, RSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Fixed</td>
</tr>
</tbody>
</table>
File Encryption Policies

This section explains the configurable options for policies affecting File Encryption agents.

Computer Policies

The following table explains the policies governing installation privileges on devices with File Encryption installed.


<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
<th>Value Range and Default</th>
</tr>
</thead>
</table>
| Allow User to Uninstall | This policy specifies whether a user other than an Administrator can uninstall the endpoint application. | Yes, No  
                          | Default: Yes                                                               |

Encryption Policies

The following table explains the policies governing how encryption is handled on File Encryption devices.

**TABLE 9-14. File Encryption Encryption Policy Descriptions**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
<th>Value Range and Default</th>
</tr>
</thead>
</table>
| Allow Secure Delete       | Specify whether to allow the user to delete files.                           | Yes, No  
                          | Default: Yes                                                               |
| Disable Optical Drive     | Disable access to CD or DVD drives.                                          | Yes, No  
<pre><code>                      | Default: No                                                               |
</code></pre>
<table>
<thead>
<tr>
<th><strong>Policy Name</strong></th>
<th><strong>Description</strong></th>
<th><strong>Value Range and Default</strong></th>
</tr>
</thead>
</table>
| Encryption Key Used | • User Key: choose a key unique to the user.  
• Group Key: choose a key unique to the group, so all users in the group will also have access to files.  
• Enterprise Key: choose a key unique to the enterprise, so all users in the enterprise will also have access to files. | User Key, Group Key, Enterprise Key  
Default: Group Key |
| Encryption Method Allowed | Choose which allowable ways to encrypt files are allowed:  
• User Key  
• Group Key  
• User-created password  
• Digital Certificates | User's Unique Key, Group Unique Key, Encrypt With Static Password, Encrypt With Certificate  
Default: All |
| Fully Encrypt Device | Specify whether all files/folders on removable media are encrypted. | Yes, No  
Default: No |
| Allow USB Devices | Specify permitted USB devices. | Any, KeyArmor  
Default: Any |
| Disable USB Drive | Disable the USB drive when not logged in, always disable, and never disable drive. | Always, Logged Out, Never  
Default: Logged Out |
| Folders to Encrypt on Removable Media | The drive letter is given and the policy value corresponds to a valid removable media device. Non-existent folders are created. If no drive letter is given then all removable media devices attached to the device at login will use the policy values. | 1-255 characters  
Default: N/A |
**Specify Folders to Encrypt**

List the folders that will be encrypted on the hard drive. Non-existent folders are created. A valid drive letter to the hard drive must also be supplied. A valid policy value is: C: \EncryptedFolder.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
<th>Value Range and Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>List the folders that will be encrypted on the hard drive. Non-existent folders are created. A valid drive letter to the hard drive must also be supplied. A valid policy value is: C: \EncryptedFolder.</td>
<td>1-255 characters</td>
</tr>
</tbody>
</table>

**Default:** %DESKTOP%

**Login Policies**

The following table explains the policies that govern logging on to the File Encryption agent.

**Table 9-15. File Encryption Login Policy Descriptions**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
<th>Value Range and Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Methods Allowed</td>
<td>Specify the allowed type(s) of authentication that can be used.</td>
<td>Fixed, ColorCode, Pin, Smart Card, RSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Fixed</td>
</tr>
<tr>
<td>Device Locked Action</td>
<td>Action to be taken when the device is locked.</td>
<td>Time Delay, Remote Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Time Delay</td>
</tr>
<tr>
<td>Failed Login Attempts Allowed</td>
<td>Number of failed logon attempts before using Lock Device Time Delay. 0 allows for unlimited attempts.</td>
<td>0-100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td><strong>Policy Name</strong></td>
<td><strong>Description</strong></td>
<td><strong>Value Range and Default</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Legal Notice Display Time</strong></td>
<td>Specify when the configured legal notice is displayed to the user.</td>
<td>Installation, Startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Startup</td>
</tr>
<tr>
<td><strong>Legal Notice Text</strong></td>
<td>Specify the body of the legal notice.</td>
<td>Insert File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>This is a sub-policy of the Legal Notice.</td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The legal notice does not appear for File Encryption 3.1.3 or older agents.</td>
</tr>
<tr>
<td><strong>Lock Device Time Delay</strong></td>
<td>Lock device for X minutes if user exceeds Failed Attempts Allowed.</td>
<td>0-999,999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

**Password Policies**

The following table explains policies governing File Encryption passwords.

**Table 9-16. File Encryption Password Policy Descriptions**

<table>
<thead>
<tr>
<th><strong>Policy Name</strong></th>
<th><strong>Description</strong></th>
<th><strong>Value Range and Default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Force Talking to Server</strong></td>
<td>Forces the File Encryption agent to communicate with the server after X amount of days. 0 makes File Encryption agent standalone.</td>
<td>0-999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 360</td>
</tr>
</tbody>
</table>
Physical Token Required

Require a physical token (smart cards) to log on to Endpoint Encryption devices.

Yes, No
Default: No

Common Policies

This section explains the configurable options for all enterprise policies affecting all Endpoint Encryption agents.

Agent Policy

The following table explains the sync interval policy.

**TABLE 9-17. Endpoint Encryption Common Agent Policy Descriptions**

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Interval</td>
<td>Specify how often (in minutes) the application communicates to PolicyServer from the device to receive updated information.</td>
<td>1-1440</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 30</td>
</tr>
</tbody>
</table>

Authentication Policies

The following table explains policies that govern authenticating local and domain user accounts.

Note

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.
### Table 9-18. Endpoint Encryption Common Authentication Policy Descriptions

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>POLICY NAME</th>
<th>DESCRIPTION</th>
<th>VALUE RANGE AND DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Allow Offline Password Change</td>
<td>Specify if users can change their password when not connected to the PolicyServer.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Local Login</td>
<td>Admin Password</td>
<td>Specify policies regarding authenticating to the local device only.</td>
<td>N/A</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Allowed Character Types</td>
<td>Specify whether passwords can contain alpha, numeric, special or a combination.</td>
<td>Alpha, Numeric, Special</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: All</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Can Contain User Name</td>
<td>Specify if the user name can be contained in the password.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Consecutive Characters Allowed</td>
<td>Specify the number of consecutive characters allowed in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Minimum Length</td>
<td>Specify the minimum length allowed for passwords.</td>
<td>0-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 6</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Password History Retention</td>
<td>Specify the number of past passwords the user is not allowed to use.</td>
<td>0-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Require How Many Characters</td>
<td>Specify the number of alpha characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Require How Many Lower Case Characters</td>
<td>Specify the number of lower case characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Category</td>
<td>Policy Name</td>
<td>Description</td>
<td>Value Range and Default</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Require How Many Numbers</td>
<td>Specify the number of numeric characters that must be used in a password.</td>
<td>0-255 Default: 0</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Require How Many Special Characters</td>
<td>Specify the number of special characters that must be used in a password.</td>
<td>0-255 Default: 0</td>
</tr>
<tr>
<td>Local Login &gt; Admin Password</td>
<td>Require How Many Upper Case Characters</td>
<td>Specify the number of upper case characters that must be used in a password.</td>
<td>0-255 Default: 0</td>
</tr>
<tr>
<td>Local Login</td>
<td>Self Help</td>
<td>Specify the policies that are used for Self Help.</td>
<td>N/A</td>
</tr>
<tr>
<td>Local Login &gt; Self Help</td>
<td>Number of Questions</td>
<td>Specify the number of questions required to be answered correctly to authenticate the user.</td>
<td>1-6 Default: 1</td>
</tr>
<tr>
<td>Local Login &gt; Self Help</td>
<td>Personal Challenge</td>
<td>Specify the personal challenge question(s) used for Self Help.</td>
<td>1-1024 Default: N/A</td>
</tr>
<tr>
<td>Local Login</td>
<td>User Password</td>
<td>Specify the policies that are used for User Passwords.</td>
<td>N/A</td>
</tr>
<tr>
<td>Local Login &gt; User Password</td>
<td>Allowed Character Types</td>
<td>Specify whether passwords can contain alpha, numeric, special or a combination.</td>
<td>Alpha, Numeric, Special Default: All</td>
</tr>
<tr>
<td>Local Login &gt; User Password</td>
<td>Can Contain User Name</td>
<td>Specify if the user name can be contained in the password.</td>
<td>Yes, No Default: Yes</td>
</tr>
<tr>
<td>Local Login &gt; User Password</td>
<td>Change Password Every</td>
<td>Specify (in days) when to force a user to change their password.</td>
<td>1-1000000 Default: 60</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>POLICY NAME</td>
<td>DESCRIPTION</td>
<td>VALUE RANGE AND DEFAULT</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Consecutive Characters Allowed</td>
<td>Specify the number of consecutive characters allowed in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Minimum Length</td>
<td>Specify the minimum length allowed for passwords.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 6</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Password History Retention</td>
<td>Specify the number of past passwords the user is not allowed to use.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Require How Many Characters</td>
<td>Specify the number of alpha characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Require How Many Lower Case</td>
<td>Specify the number of lower case characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td>Characters</td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Require How Many Numbers</td>
<td>Specify the number of numeric characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Require How Many Special Characters</td>
<td>Specify the number of special characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>Require How Many Upper Case</td>
<td>Specify the number of upper case characters that must be used in a password.</td>
<td>0-255</td>
</tr>
<tr>
<td>User Password</td>
<td>Characters</td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Local Login &gt;</td>
<td>User Name Case Sensitive</td>
<td>Specify if the user name is case sensitive</td>
<td>Yes, No</td>
</tr>
<tr>
<td>User Password</td>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>POLICY NAME</td>
<td>DESCRIPTION</td>
<td>VALUE RANGE AND DEFAULT</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Network Login</td>
<td>Distinguished Name</td>
<td>Optional: Specify the distinguished name of the authentication server. If no Distinguished Name is specified, this will default to the LDAP server Default Naming Convention.</td>
<td>1-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Network Login</td>
<td>Domain Authentication</td>
<td>Specifies if the Windows credentials should be used to authenticate.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Network Login</td>
<td>Domain Name</td>
<td>NetBIOS name of the domain for Single Sign On. Default is NetBIOS value used by the PolicyServer.</td>
<td>1-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Network Login</td>
<td>Host Name</td>
<td>Specify the host name. The host name can be a domain name.</td>
<td>1-255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Network Login</td>
<td>Port Number</td>
<td>Optional: 0 = use default. Specifies the port to be used for the connection. If no port number is specified, the LDAP provider uses the default port number.</td>
<td>0-65535</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Network Login</td>
<td>Server Type</td>
<td>Type of server used to authenticate client user requests.</td>
<td>LDAP, LDAPProxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: LDAP</td>
</tr>
<tr>
<td>Authentication</td>
<td>Remember User Between Login</td>
<td>Remember last used user name and display it in the authentication screen.</td>
<td>Yes, No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: Yes</td>
</tr>
</tbody>
</table>
Groups in PolicyServer MMC

Endpoint Encryption utilizes both role-based and identity-based authentication to secure data. Correctly configuring Endpoint Encryption groups ensures that data remains encrypted from unauthorized users, thus preventing data loss risk from accidental information release or deliberate sabotage.

Topics include:

• *About Groups* on page 10-2
• *Group Management* on page 10-2
• *Offline Groups* on page 10-12
About Groups

Groups are managed in PolicyServer MMC. The following table describes the types of groups available.

TABLE 10-1. PolicyServer Group Types

<table>
<thead>
<tr>
<th>GROUP</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Group</td>
<td>The highest level of groups under the Enterprise. Each Top Group has a unique node underneath the Enterprise.</td>
</tr>
<tr>
<td>Subgroup</td>
<td>Groups created within a Top Group. A subgroup inherits the policies of its parent group.</td>
</tr>
<tr>
<td></td>
<td>• Policy inheritance only occurs when a subgroup is created</td>
</tr>
<tr>
<td></td>
<td>• Policy changes to a top level group do not filter down to existing subgroups</td>
</tr>
<tr>
<td></td>
<td>• Subgroup policies cannot be more permissive than the parent groups</td>
</tr>
</tbody>
</table>

Note

Although subgroups inherit all existing policies of the parent group, you must separately add users and devices to the subgroup. Adding Endpoint Encryption users to a subgroup does not automatically add the users to the Top Group. However, you can add users to both the Top Group and subgroup.

Group Management

This section explains how to use PolicyServer MMC to add new groups, add or remove Endpoint Encryption users and devices, and modify groups.
Adding a Top Group

Groups simplify managing Endpoint Encryption agents, users, policies, subgroups, and devices. A Top Group is the highest level group.

**Note**

It is not possible to add the Enterprise Administrator or Enterprise Authenticator accounts to groups. To create a Group Administrator, add a user and change the account permissions within the group. For more information, see *Modifying a User on page 11-9*.

**Procedure**

1. Right-click the Enterprise in the left pane, then click **Add Top Group**.

![Add Top Group Screen](image)

**FIGURE 10-1. Add Top Group Screen**

The **Add New Group** screen appears.

2. Specify the name and description for the group.

3. If using Endpoint Encryption devices that do not support Unicode, select **Support Legacy Devices**.

**Note**

Some legacy devices may not be able to communicate with PolicyServer using Unicode. Assign Unicode and legacy Endpoint Encryption devices to different groups.
4. Click **Apply**.

5. At the confirmation message, click **OK**.

   The new group is added to the tree structure in the left pane.

---

**Adding a Subgroup**

Although subgroups inherit all existing policies of the parent group, you must separately add users and devices to the subgroup.

---

**Procedure**

1. Right-click a group in the left pane tree structure, and then click **Add**.

   The **Add New Group** window appears.

2. Follow the steps in *Adding a Top Group on page 8-6*.

   The new group is added to the tree structure inside the Top Group.
Modifying a Group

**Procedure**

1. Right-click a group in the left pane tree structure, then click **Modify**.
   The **Modify Group** screen appears.
2. Specify changes.
3. Click **Apply**.

Removing a Group

Use the tree structure to remove a group. Removing a Top Group removes all subgroups.

**Procedure**

1. Right-click a group in the left pane tree structure, then click **Remove**.
   A warning message appears.
2. Click **Yes** to remove the group.
   The selected group no longer appears in the tree structure.

Adding a New User to a Group

**Note**
Adding a user to the Enterprise does not assign the user to any groups
Adding a user to a group adds the user to the group and to the Enterprise
Procedure

1. Expand the group and open **Users**.

2. Go to the right pane and right-click the whitespace, then select **Add New User**.

   The **Add New User** screen appears.

3. Specify the following options:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the user name for the new user account (required).</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the first name for the new user account (required).</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the last name for the new user account (required).</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>Specify the employee ID for the new user account (optional).</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log devices.</td>
</tr>
<tr>
<td>Group User Type</td>
<td>Select the privileges of the new account.</td>
</tr>
</tbody>
</table>

**Note**
For information about account roles, see *Endpoint Encryption User Roles on page 2-5*.

Options include:
- User
- Authenticator
- Administrator

**Note**
It is not possible to add Enterprise Administrator or Enterprise Authenticator accounts to groups.

<table>
<thead>
<tr>
<th><strong>One Group</strong></th>
<th>Select whether the new user account is allowed to be a member of multiple group policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Select the method that the new user account uses to log on to Endpoint Encryption devices.</td>
</tr>
</tbody>
</table>

**Note**
The default authentication method for users is **None**.

For information about account roles, see *Devices and Users Overview on page 2-1*.

---

4. **Click OK.**

The new user is added to the selected group and to the Enterprise. The user can now log on to Endpoint Encryption devices.
Adding an Existing User to a Group

A user can be a member of multiple groups.

Procedure

1. Expand the group in the left pane, then click Users.

2. Go to the right pane and right-click the whitespace, then select Add Existing User.

The Add Users To Group screen appears.

3. Specify user details and then click Search.
The **Source** field populates with any accounts that match the search criteria.

4. Select users from the **Source** list and click the blue arrow to add them.

For information about search icons, see *Add/Remove Search Result Icons on page 11-15.*

The selected user moves to the **Destination** list.

5. To change a user password:
   a. In the **Destination** list, highlight the user.
   b. Click **Enter User Password** located at the bottom of the window.
   c. In the window that appears, specify the user’s authentication method.
   d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

---

**Removing Users From a Group**

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user account. Otherwise, only the Enterprise Administrator or Enterprise Authenticator accounts can make changes to the group.

Removing a user from a group restricts the user from accessing any Endpoint Encryption device assigned to that group. Before removing Endpoint Encryption users, make sure that the users have backed up and unencrypted their data.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove User**.
A warning message appears.

3. To remove the user from the Enterprise as well, select **Remove from Enterprise**.

---

**Note**
Removing a user from the Enterprise also removes that user from all groups and subgroups.

---

4. Click **Yes**.

   The user is removed.

---

### Removing All Users From a Group

---

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user. Otherwise, only Enterprise Administrator and Enterprise Authenticator accounts can make group-level changes.

---

**Procedure**

1. Expand the group, then click **Users**.

2. In the right pane, right-click the user and select **Remove All Users**.

   A warning message displays.

3. To remove all users from the Enterprise as well, select **Remove from Enterprise**.

---

**Note**
Removing a user from the Enterprise also removes that user from all groups and subgroups.

---

4. Click **Yes**.
Adding a Device to a Group

**Note**

Each Endpoint Encryption device can belong to only one group.

**Procedure**

1. In the left pane, expand the desired policy group and click **Devices**.
2. In the right pane, right-click the whitespace and select **Add Device**.
   - The **Add Devices to Group** screen appears.

3. Type the device details, then click **Search**.
   - If there is a match, the **Source** field populates with Endpoint Encryption devices.
4. Select applicable Endpoint Encryption devices from the **Source** field, then click the **blue arrow** to add them.
   - For information about search icons, see *Add/Remove Search Result Icons on page 11-15*. 

![Figure 10-5. Add Devices to Group Screen](image)
Click **Apply** to add the Endpoint Encryption device to the selected group.

The Endpoint Encryption device is added to the group.

---

### Removing a Device from a Group

Removing a device from a group removes the device from the selected group only.

---

**WARNING!**

To remove a device from all groups, remove it from the Enterprise. Before deleting a device from the Enterprise, verify that the device has been unencrypted and that all Endpoint Encryption agents were uninstalled. Failure to do so may result in irreversible data loss.

---

**Procedure**

1. Expand the group, then open **Devices**.

2. In the right pane, right-click the device and select **Remove Device**.

   A warning message appears.

3. Click **Yes**.

   The device is removed.

---

### Offline Groups

An offline group is a group of endpoints that did not connect to PolicyServer when the File Encryption agent was installed. Export the policies, users, and devices for that group to a file and install them on each endpoint. When the group requires changes, export a new file and repeat the import.

Policies are automatically updated when the agent connects to PolicyServer.
Creating an Offline Group

Offline groups allow agents that do not need to or cannot communicate with PolicyServer to get updated policies. The Endpoint Encryption agent installation files must be available to the server where PolicyServer is installed.

Note

Exported groups must contain at least one user. The group name must also be alphanumeric only.

Procedure

1. From the left pane, right-click the group and then select Export.

The PolicyServer Export Group Wizard appears.

2. Select Create off-line devices.

FIGURE 10-6. PolicyServer Exporting Group Wizard
3. Specify the export location.

4. Specify and confirm the export password.

---

**Note**

The export password is used to authenticate the executable on the agent.

---

5. Click **Next**

6. Click **Add** to browse to and upload Endpoint Encryption client installers.

**TABLE 10-2. Endpoint Encryption Installation Filename**

<table>
<thead>
<tr>
<th>INSTALLATION FILE</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileEncryptionIns.exe</td>
<td>Installs the File Encryption agent.</td>
</tr>
</tbody>
</table>

---

**Note**

For older Endpoint Encryption product versions, see the supporting documentation.

---

7. Click **Next**.

8. Depending on the license type, specify the number of devices to be installed on. The number of licenses available is reduced with every device.

9. Optionally specify a **Device Name Prefix**. PolicyServer uses the device prefix number to generate a unique Device ID and device encryption key for each device in this group.

10. Click **Next**.

    The offline group build begins.

11. Click **Done** to generate the export file at the specified location.

    A generated executable file named “Export” is created on the desktop. Use this to distribute policy changes to offline groups.
Updating an Offline Group

The following procedure explains how to create an update for an offline group.

Procedure

1. From the left pane, right-click the group, then select **Export**.
   
   The **PolicyServer Export Group Wizard** opens.

2. Select **Update off-line devices**.

3. Specify the export password.

   **Note**
   
   Use the export password to authenticate the executable on the Endpoint Encryption agent.

4. Click **Browse** to specify a location to store the export file.

5. Click **Next**
   
   The offline group build begins.

6. Click **Done**.
   
   The export file is generated at the specified location.

7. Install the software on the device using the generated executable or script.

   **Note**
   
   See the **Endpoint Encryption Installation and Migration Guide**.
Chapter 11

Users in PolicyServer MMC

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Control Manager or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

Note
For a description of Endpoint Encryption user roles and authentication, see Endpoint Encryption Users on page 2-4.

This chapter explains account roles and authentication methods, how to administer PolicyServer MMC to manage policies affecting Endpoint Encryption users, and how to control information access by using the Users policy node in PolicyServer MMC. This chapter also explains how to restore deleted Endpoint Encryption users.

Topics include:

• Adding Users to Endpoint Encryption on page 6-4
• Finding a User on page 11-8
• Modifying a User on page 11-9
• Adding a New User to a Group on page 8-8
• Adding an Existing User to a Group on page 8-13
• Changing a User's Default Group on page 11-15
• Allowing User to Install to a Group on page 11-16
• Removing Users From a Group on page 10-9
• Removing All Users From a Group on page 10-10
• Restoring a Deleted User on page 6-25
• Working with Passwords on page 6-11
Adding Users to Endpoint Encryption

Endpoint Encryption has several options to add users to Endpoint Encryption:

• Add users manually, one at a time
• Bulk import numerous users with a CSV file
• Use the External Directory Browser with Active Directory

Adding a New Enterprise User

The following procedure explains how to add new Endpoint Encryption users to the Enterprise.

**Note**

Adding a new Endpoint Encryption user to the Enterprise does not assign the user to any groups.

Adding a new Endpoint Encryption user to a group adds the user to the group and to the Enterprise.

**Procedure**

1. To access Enterprise Users, do one of the following:
   • Expand the Enterprise, then open **Enterprise Users**.
   • Expand the Enterprise, expand the group, then open **Users**.

2. Right-click the white space in the right pane and select **Add User**.
The **Add New User** screen displays.

![Add New User screen](image)

**Figure 11-1. Add New User screen**

3. Specify the following options:

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the user name for the new user account (required).</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the first name for the new user account (required).</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the last name for the new user account (required).</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>Specify the employee ID for the new user account (optional).</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on to devices.</td>
</tr>
<tr>
<td>Group User Type</td>
<td>Select the privileges of the new account. For information about account roles, see <em>Devices and Users Overview on page 2-1</em>. Options include:</td>
</tr>
</tbody>
</table>
Users in PolicyServer MMC

<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• User</td>
<td></td>
</tr>
<tr>
<td>• Authenticator</td>
<td></td>
</tr>
<tr>
<td>• Administrator</td>
<td></td>
</tr>
</tbody>
</table>

Note
It is not possible to add Enterprise Administrator or Authenticator accounts to groups.

<table>
<thead>
<tr>
<th>One Group</th>
<th>Select whether the new user account is allowed to be a member of multiple group policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>Select the method that the new user account uses to log on to Endpoint Encryption devices. For information about authentication methods, see Devices and Users Overview on page 2-1.</td>
</tr>
</tbody>
</table>

Note
The default authentication method for users is None.

4. Click OK.

The new Endpoint Encryption user is added to the Enterprise. The user cannot log on to Endpoint Encryption devices until the user account is added to a group.

Importing Users from a CSV File

Use a Comma Separated Values (CSV) file to simultaneously import multiple users.

Format: user name (required), first name, last name, employee ID, email address

Note
Include a comma for fields with no data.

Make sure to create one CSV file for each group of users to import. All users in the CSV file are added to the same group.
Procedure

1. Expand the group in the left pane, then click **Users**.
2. Right-click whitespace in the right pane, then select **Bulk Import Add Users**. 
   The open file window appears.
3. Go to the CSV file and click **Open**.
4. At the confirmation, click **OK**.
   The users in the CSV file are added to the group and the Enterprise.

---

Importing Active Directory Users

PolicyServer maintains a user directory separate from the Active Directory database. This allows PolicyServer absolute security over access to all Endpoint Encryption devices, user rights, and authentication methods.

For information about configuring Active Directory integration, see the *Endpoint Encryption Installation and Migration Guide*.

---

Procedure

1. Log on to PolicyServer MMC.
2. Open **Enterprise Users**, right-click the right pane (whitespace) and then select **External Directory Browser**.
   The **Active Directory User Import** screen appears.
3. Go to **Edit > Connect to Domain**.
The **Add Server** screen appears.

![Add Server Screen](image)

4. Specify the following parameters for the Active Directory LDAP Server:
   - **Host name**
   - **Port**
   - **User name**
   - **Password**

5. Click **OK**.

6. Wait for the specified Active Directory domain to populate.
   The Active Directory tree for the specified domain appears in the left pane.

7. From the left pane, use the navigation tree to select the container from which to add users.
   The available users populate in the right pane.

8. Select applicable users, right-click the selection and then select:
   - **Add to Enterprise**
   - **Add to Group**
     a. Expand the Enterprise.
     b. Select the appropriate group.
c. Click **OK**.

9. Click **OK** to add the users to the specified location.
   A confirmation window appears.

10. Click **OK** to confirm.
    An import status message displays.

11. Click **OK** to finish, or repeat the procedure to select more users to import

---

**Finding a User**

It is faster to search for users at the group level; however, this is at the cost of searching the entire Enterprise.

---

**Procedure**

1. From the left pane, click **Enterprise Users** or expand the group and then click **Users**.

2. At the upper corner of the right pane, click **Search**.
The User Search Filter window appears.

![User Search Filter Window](image)

**FIGURE 11-2. User Search Filter window**

3. Specify search details and then click **Search**.

All accounts matching the search criteria appear.

---

**Note**

If there are many users, use **Page Counter** to go from one page to another or click **Clear** to remove all results.

---

**Modifying a User**

Any Group Administrator can change a user's profile information.
Note

- Enterprise-level changes are applied to the user universally, but group-level changes apply only to that group.

Procedure

1. Open Enterprise Users.
2. In the right pane, right-click the user and then select Modify User.
   
   The Modify User screen appears.
3. Make the necessary changes. If the authentication method changes to Fixed Password, provide the default user password.
4. Click OK.
5. At the confirmation message, click OK.

Viewing a User's Group Membership

List groups to view the Endpoint Encryption user's group membership. If a user belongs to multiple groups, you can also change the priority of assigned groups. For information about the default group, see Changing a User's Default Group on page 11-15.

Procedure

1. Open Enterprise Users.
2. Right-click the user, then select List Groups.
   
   The Group Membership list appears.
Adding a New User to a Group

**Note**

Adding a user to the Enterprise does not assign the user to any groups.

Adding a user to a group adds the user to the group and to the Enterprise.

**Procedure**

1. Expand the group and open **Users**.

2. Go to the right pane and right-click the whitespace, then select **Add New User**.

   The **Add New User** screen appears.

3. Specify the following options:

   ![Add New User Screen](image)

   **FIGURE 11-3. Add New User Screen**

   Specify the following options:
<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Specify the user name for the new user account (required).</td>
</tr>
<tr>
<td>First name</td>
<td>Specify the first name for the new user account (required).</td>
</tr>
<tr>
<td>Last name</td>
<td>Specify the last name for the new user account (required).</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>Specify the employee ID for the new user account (optional).</td>
</tr>
<tr>
<td>Freeze</td>
<td>Select whether to temporarily disable the new user account (optional). While</td>
</tr>
<tr>
<td></td>
<td>frozen, the user is unable to log devices.</td>
</tr>
<tr>
<td>Group User Type</td>
<td>Select the privileges of the new account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For information about account roles, see <em>Endpoint Encryption User Roles on</em>*</td>
</tr>
<tr>
<td></td>
<td><em>page 2-5.</em></td>
</tr>
<tr>
<td></td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td>• Authenticator</td>
</tr>
<tr>
<td></td>
<td>• Administrator</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>It is not possible to add Enterprise Administrator or Enterprise Authenticator</td>
</tr>
<tr>
<td></td>
<td>accounts to groups.</td>
</tr>
<tr>
<td>One Group</td>
<td>Select whether the new user account is allowed to be a member of multiple group</td>
</tr>
<tr>
<td></td>
<td>policies.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Select the method that the new user account uses to log on to Endpoint</td>
</tr>
<tr>
<td></td>
<td>Encryption devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The default authentication method for users is <strong>None</strong>.</td>
</tr>
<tr>
<td></td>
<td>For information about account roles, see <em>Devices and Users Overview on</em>*</td>
</tr>
<tr>
<td></td>
<td><em>page 2-1.</em></td>
</tr>
</tbody>
</table>
4. Click **OK**.

The new user is added to the selected group and to the Enterprise. The user can now log on to Endpoint Encryption devices.

---

**Adding an Existing User to a Group**

A user can be a member of multiple groups.

**Procedure**

1. Expand the group in the left pane, then click **Users**.

2. Go to the right pane and right-click the whitespace, then select **Add Existing User**.
The Add Users To Group screen appears.

![Add Users To Group Screen]

**Figure 11-4. Add Users To Group Screen**

3. Specify user details and then click **Search**.

   The **Source** field populates with any accounts that match the search criteria.

4. Select users from the **Source** list and click the blue arrow to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 11-15*.

   The selected user moves to the **Destination** list.

5. To change a user password:
   
   a. In the **Destination** list, highlight the user.
b. Click **Enter User Password** located at the bottom of the window.

c. In the window that appears, specify the user's authentication method.

d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

### Add/Remove Search Result Icons

<table>
<thead>
<tr>
<th><strong>CENTER ICONS</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Add a single selected item to <strong>Destination</strong> field.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Add all found items based on search criteria to <strong>Destination</strong> field.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Remove a single selected item from <strong>Destination</strong> field.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Remove all items from <strong>Destination</strong> field.</td>
</tr>
</tbody>
</table>

### Changing a User’s Default Group

Endpoint Encryption users can belong to any number of groups while Endpoint Encryption devices can only belong to one group. The default group is the group that controls the user's policies. The first group listed in the group membership is the default group for the user.
Note
The user must be allowed to install to the default group. For more information, see "Allowing User to Install to a Group on page 11-16."

Procedure

1. Open Enterprise Users.
2. Right-click the user and then select List Groups.
   The Group Membership list appears.
3. Right-click the user and then select Move to top.
   The user’s default group is changed.

Allowing User to Install to a Group

Allowing a user to install to a group allows users to install Endpoint Encryption devices to a group that they are a member, without requiring the additional privileges of the Administrator or Authenticator role.

Note
The default setting is Disallow User To Install To This Group.

Procedure

1. Open Enterprise Users.
2. Right-click the user and then select List Groups.
   The Group Membership list appears.
3. Right-click the user and then select Allow User To Install To This Group.
The user can now install devices to this group.

Removing Users From a Group

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user account. Otherwise, only the Enterprise Administrator or Enterprise Authenticator accounts can make changes to the group.

Removing a user from a group restricts the user from accessing any Endpoint Encryption device assigned to that group. Before removing Endpoint Encryption users, make sure that the users have backed up and unencrypted their data.

**Procedure**

1. Expand the group, then click **Users**.

2. In the right pane, right-click the user and select **Remove User**.
   
   A warning message appears.

3. To remove the user from the Enterprise as well, select **Remove from Enterprise**.

   **Note**
   
   Removing a user from the Enterprise also removes that user from all groups and subgroups.

4. Click **Yes**.

   The user is removed.
Removing All Users From a Group

**WARNING!**
Before removing a Group Administrator or Group Authenticator account, reassign this role to another user. Otherwise, only Enterprise Administrator and Enterprise Authenticator accounts can make group-level changes.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove All Users**.
   A warning message displays.
3. To remove all users from the Enterprise as well, select **Remove from Enterprise**.
   
   **Note**
   Removing a user from the Enterprise also removes that user from all groups and subgroups.
4. Click **Yes**.

Restoring a Deleted User

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption user.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the **Recycle Bin**.
3. Open **Deleted Users**.
The right pane loads all deleted users.

4. Right-click the user account, then select **Restore User**.

The user is added back to the Enterprise, but does not belong to any policy groups.

---

**Working with Passwords**

When a user forgets the password or misplaces an endpoint, the user can reset the password using methods defined by policies. The following password reset methods are available:

- Microsoft Windows Active Directory
- Control Manager
- PolicyServer MMC
- Remote Help
- Self Help

All of these options involve setting the policy at the Enterprise or at the group/policy level, if necessary. Use the Support Information policy to provide support-related information to users about password resets.

---

**Note**

For information about configuring support information in Control Manager, see *Endpoint Encryption Policy Settings on page 5-12*.

For information about configuring support information in PolicyServer MMC, see *Support Information Setup on page 11-29*.
Resetting an Enterprise Administrator/Authenticator Password

Only Enterprise Administrator accounts can reset an Enterprise Administrator password. An Authenticator within the same group permissions or higher, can reset an Administrator or Authenticator password within that group.

---

**Tip**

As a safeguard against password loss, Trend Micro recommends having at least three Enterprise Administrator accounts at all times. If an Enterprise Administrator account password is lost, use Self Help authentication to reset the password.

---

**Procedure**

1. Log on to PolicyServer MMC using an Enterprise Administrator account.

2. Open **Enterprise Users**.

3. Right-click the Enterprise Administrator or Authenticator account with the lost password, then select **Change Password**.

   The **Change Password** window appears.

4. Select an authentication method.

5. Specify the password (if requested).

6. Click **Apply**.

   The account password is reset.

---

**Note**

The **User must change password at next logon** option is only available after the agent updates policies.
Resetting a Group Administrator/Authenticator Password

Changes to passwords only affect the selected group. To reduce the number of passwords, assign Group Administrator accounts to only one Top Group.

Procedure

1. Log on to PolicyServer MMC using a Group Administrator account.
2. Expand the group, then click Users.
3. Right-click the Group Administrator or Group Authenticator account with the lost password, then select Change Password.

   The Change Password window appears.
4. Select an authentication method.
5. Specify and confirm the password (if requested).
6. Click Apply.

   The account password is reset.

---

Note

The User must change password at next logon option is only available after the client updates.

---

Resetting User Passwords

When resetting a user’s password, select the User must change password at next logon check box to require a user to change the password at next logon. The user will be required to change the password after logging on any Endpoint Encryption device.

---

Tip

Trend Micro recommends using domain authentication.
Resetting to a Fixed Password

Procedure

1. Open Enterprise Users or expand the group, then click Users.
2. Select the user accounts from the right pane.

   **Note**
   Hold SHIFT to select multiple users. Multiple selection is only available at the group level.

3. Right-click and select Change Password.
   The Change Password window appears.

4. For the Authentication Method, select Fixed Password.
5. Specify and confirm the password.
6. Click Apply.
   The user must change his/her password after successfully logging on Endpoint Encryption devices.

Resetting a User Password with Active Directory

Trend Micro recommends using Active Directory to reset the user password, especially if the user has access to the company Help Desk, has network connectivity, or if Windows Single Sign-on (SSO) is enabled.

Refer to the appropriate operating system user guide for more information about resetting a domain user password using Active Directory.
Smart Card

Smart card authentication requires both a PIN and a physical token to confirm the user identity. To use smart card authentication, make sure that the following requirements are met:

• The smart card reader is connected to the endpoint and the smart card is inserted into the smart card reader.

• ActivClient 6.1 with all service packs and updates are installed.

• Specify the smart card PIN in the password field.

**WARNING!**

Failure to provide a correct password sends a password error and may result in locking the smart card.

---

**Note**

Smart card authentication is only configurable with PolicyServer MMC.

Enable smart card authentication for each Endpoint Encryption agent:

• For File Encryption, go to Login > Password > Physical Token Required.

• For Full Disk Encryption, go to Full Disk Encryption > Login > Token Authentication

**Smart Card Registration**

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

Use one of the following methods to register a smart card:

• To use the Full Disk Encryption preboot, see Registering a Smart Card in Full Disk Encryption Preboot on page 11-25.
To use PolicyServer MMC, see *Configuring Smart Card Authentication in PolicyServer MMC on page 11-24*.

### Configuring Smart Card Authentication in PolicyServer MMC

Registering a smart card allows a user to log on with smart card authentication. For information about Full Disk Encryption Preboot smart card authentication, see *File Encryption Smart Card Authentication on page 13-4*.

**Procedure**

1. Log on to PolicyServer MMC.
2. Go to Full Disk Encryption > Login.
3. Right-click **Token Authentication** and select **Enable**.
4. Go to Full Disk Encryption > Password.
5. Right-click **Authentication Methods Allowed**, then select **Properties**.

   The *Edit Policy Value* window appears.

6. Select **PIN**, then click **OK** to confirm the policy change.

Smart card authentication is enabled.

### Registering a Smart Card in PolicyServer MMC

Before proceeding, make sure to configure smart card authentication. For information about configuring smart card authentication, see *Configuring Smart Card Authentication in PolicyServer MMC on page 11-24*.

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.
After assigning a smart card PIN to the user, the user can log on the Full Disk Encryption agent directly with the smart card from the smart card authentication screen in the Full Disk Encryption preboot.

**Procedure**

1. Log on to PolicyServer MMC.
2. Insert the smart card in the reader.
3. Connect the reader to the PolicyServer endpoint.
4. Expand the specific group and then click Users.
5. Right-click a user and then select Change Password.

   The Change Password window appears.

6. In the Authentication Method drop-down, select Smart Card.
7. Specify and confirm the PIN.
8. In the Select a slot drop-down, select the smart card type.
9. Click Apply to confirm token authentication.
10. Click OK to confirm the user account changes.

The smart card is registered to all users in the same group as the selected user.

**Registering a Smart Card in Full Disk Encryption Preboot**

**Procedure**

1. Follow the instructions to change passwords, then select Smart Card.

   See Resetting User Passwords on page 11-21.
2. Insert the smart card in the reader.
3. Connect the reader to the endpoint.
4. Specify the user name and fixed password.

5. Click **Continue**.

6. At the confirmation message, click **Continue**.

7. At the **Register Token** window, do the following:
   a. Type the new PIN provided by the Group or Enterprise Administrator.
   b. Confirm the new PIN.
   c. Select the smart card type from the **Token** drop-down list.
   d. Click **Continue** to finish registering the smart card token.

---

**Using Self Help Password Reset**

Users who have forgotten their passwords can use Self Help to authenticate without Help Desk assistance. Use the Number of Questions and the Personal Challenge policies to set the number of personal challenge questions and the questions that the user must answer, respectively. Self Help questions are answered during the initial user authentication and when users change their passwords.

For information about using Self Help, see *Self Help on page 2-12*.

---

**Note**

Self Help requires that the Endpoint Encryption agent has network connectivity to PolicyServer.

---

**Procedure**

1. Expand **Enterprise Policies** or expand the group and then expand **Policies**.

2. Go to **Common** > **Authentication** > **Local Login** > **Self Help**.
3. Open **Number of Questions** to set the required number of questions that users must answer.

- **WARNING!**
  Do not set **Number of Questions** greater than six. Otherwise, users are unable to authenticate using Self Help.

4. Right-click **Personal Challenge** and select **Add** to set a question that the user must answer. Repeat until all personal challenge questions are defined.

   The user will be prompted to set the personal challenge question answers the next time that the user logs on any Endpoint Encryption device.

---

**Remote Help Assistance**

Remote Help allows users to reset a forgotten password or locked account. Any Endpoint Encryption user who has a locked account or forgot the account password must reset the password before being able to log on to any Endpoint Encryption device. Remote Help requires that the user contact the Help Desk for a Challenge Response. Remote Help does not require network connectivity to PolicyServer.
Procedure

1. Log on to PolicyServer MMC using any account with Group Administrator permissions in the same policy group as the user.

2. Ask the user to go to Help > Remote Help from the Endpoint Encryption agent.

3. Ask the user for the Device ID.

4. In PolicyServer MMC, open Enterprise Devices or expand the user's group and open Devices.

5. In the right pane, right-click the user's device and then select Soft Token.

   The Software Token window appears.

6. Get the 16-digit challenge code from the user, and type it into the Challenge field of the Software Token window.
7. Click **Get Response**.
   The **Response** field loads with an 8-character string.

8. Tell the user the 8-character string from the **Response** field.

9. The user inputs the string in the **Response** field on the endpoint and clicks **Login**.

10. The user must specify a new password.

---

**Support Information Setup**

The Support Information policy specifies information about the organization's Support Help Desk. You can uniquely configure the Support Information policy for each group.

**Procedure**

1. Log on to PolicyServer MMC with either an Enterprise Administrator/Authenticator account or a Group Administrator/Authenticator account within the same policy group as the user.

2. Expand the user's group and go to **Policies > Full Disk Encryption > Login**.

3. Right-click the **Support Info** policy and select **Add**.

4. Specify support information.
5. Click **OK**.

---

**Using Remote Help to Unlock Full Disk Encryption Devices**

**Important**

- Restarting the Endpoint Encryption device resets the challenge code.
- Manually synchronizing policies with PolicyServer also resets the challenge code.
- The challenge code and response code are not case sensitive.

**Procedure**

1. From the Full Disk Encryption preboot, go to **Menu > Authentication > Remote Help**.
2. Provide the **Challenge Code** to the Policy/Group Administrator.
3. Specify the **Response Code** provided by the Policy/Group Administrator.
4. Click **Login**.
   
   The **Change Password** screen appears.

**Note**

If the account uses domain authentication, the endpoint boots directly into Windows.

5. Specify and confirm new password, then click **Next**.
   
   The device boots into Windows.

---

**Using Remote Help to Unlock a File Encryption Device**

If a user exceeds the number of authentication attempts and policies are set to enact Remote Authentication, File Encryption locks Endpoint Encryption folders and notifies
the user that Remote Help is required. Using Remote Help to unlock File Encryption requires assistance from the Enterprise Authenticator or Group Authenticator.

---

**Note**

For information about using Remote Help, see *Remote Help on page 2-11*.

---

**Procedure**

1. Right-click the File Encryption tray icon, then select **Remote Help**.

   The **Remote Help** screen appears.

   ![Remote Help Screen](image)

   **FIGURE 11-7. File Encryption Remote Help**

2. Specify the user name.

3. Click **Get Challenge**.

4. Type the **Response** provided by the Enterprise/Group Authenticator.
5. Click **Log In**.

The user is authenticated to File Encryption and a notification displays.
Devices in PolicyServer MMC

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

This chapter explains how to administer PolicyServer MMC to manage policies affecting Endpoint Encryption devices, and how to ensure data security by using the specialized Endpoint Encryption devices widget. This chapter also explains how to restore deleted Endpoint Encryption devices.

Topics include:

- Adding a Device to a Group on page 10-11
- Removing a Device from a Group on page 10-12
- Deleting a Device from the Enterprise on page 12-5
- Getting the Software Token on page 12-6
- Using the Recovery Key on page 12-7
- Viewing Device Attributes on page 12-8
- Viewing Directory Listing on page 12-11
- Viewing Group Membership on page 12-11
• Killing a Device on page 12-12
• Locking a Device on page 12-12
• Resetting a Device on page 12-13
• Restoring a Deleted Device on page 7-17
Adding a Device to a Group

Note

Each Endpoint Encryption device can belong to only one group.

Procedure

1. In the left pane, expand the desired policy group and click Devices.
2. In the right pane, right-click the whitespace and select Add Device.

The Add Devices to Group screen appears.

3. Type the device details, then click Search.

If there is a match, the Source field populates with Endpoint Encryption devices.

4. Select applicable Endpoint Encryption devices from the Source field, then click the blue arrow to add them.

For information about search icons, see Add/Remove Search Result Icons on page 11-15.
5. Click **Apply** to add the Endpoint Encryption device to the selected group.

The Endpoint Encryption device is added to the group.

---

**Add/Remove Search Result Icons**

<table>
<thead>
<tr>
<th>CENTER ICONS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon1.png" alt="Icon" /></td>
<td>Add a single selected item to <strong>Destination</strong> field.</td>
</tr>
<tr>
<td><img src="icon2.png" alt="Icon" /></td>
<td>Add all found items based on search criteria to <strong>Destination</strong> field.</td>
</tr>
<tr>
<td><img src="icon3.png" alt="Icon" /></td>
<td>Remove a single selected item from <strong>Destination</strong> field.</td>
</tr>
<tr>
<td><img src="icon4.png" alt="Icon" /></td>
<td>Remove all items from <strong>Destination</strong> field.</td>
</tr>
</tbody>
</table>

**Removing a Device from a Group**

Removing a device from a group removes the device from the selected group only.

---

**WARNING!**

To remove a device from all groups, remove it from the Enterprise. Before deleting a device from the Enterprise, verify that the device has been unencrypted and that all Endpoint Encryption agents were uninstalled. Failure to do so may result in irreversible data loss.

---

**Procedure**

1. Expand the group, then open **Devices**.
2. In the right pane, right-click the device and select **Remove Device**.

   A warning message appears.

3. Click **Yes**.

   The device is removed.

### Deleting a Device from the Enterprise

Deleting any Endpoint Encryption device from the Enterprise also removes the device from all policy groups. The deleted Endpoint Encryption device continues functioning as long as connectivity and password policies are current on the device. However, Endpoint Encryption users cannot recover files if the Endpoint Encryption device has a critical hardware failure after it has been removed from the Enterprise. To mitigate this risk, immediately decrypt the Endpoint Encryption device and uninstall the Endpoint Encryption agent software.

---

**WARNING!**

Make sure to decrypt the device (files or hard disk) and uninstall the Endpoint Encryption agent before deleting a device from the Enterprise. Failure to do so may result in data loss.

For information about removing a device from a specific group, but not the Enterprise, see *Removing a Device from a Group on page 10-12*.

### Procedure

1. Uninstall the Endpoint Encryption agent from the endpoint.

   **Note**

   For information about uninstalling Endpoint Encryption agents, see the *Endpoint Encryption Installation and Migration Guide*.

2. Open **Enterprise Devices**.

3. In the right pane, right-click the device and select **Delete Device**.
4. At the warning message, click **Yes** to confirm.

The Endpoint Encryption device is deleted from the Enterprise.

---

**Note**

For information about adding the Endpoint Encryption device back the Enterprise, see *Restoring a Deleted Device on page 7-17*.

---

**Getting the Software Token**

Generating a “software token” creates a unique string that you can use to unlock Endpoint Encryption devices and to remotely help Endpoint Encryption users reset forgotten passwords.

For information about resetting passwords or unlocking a user account, see *Remote Help Assistance on page 11-27*.

---

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. Right-click the device and select **Soft Token**.

   The **Software Token** screen appears.

3. Get the 16-digit challenge code from the user, and type it into the **Challenge** field of the **Software Token** window.

4. Click **Get Response**.

   The **Response** field loads with an 8-character string.

5. Tell the user the 8-character string from the **Response** field.
The Endpoint Encryption device is unlocked and the Endpoint Encryption user can log on to the device.

## Using the Recovery Key

Generating a “recovery key” allows the user to decrypt a hard disk when the user has forgotten the original password or key. The recovery key is only available to Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker agents because they do not use the other recovery methods available in Full Disk Encryption.

**Note**

The recovery key is used for encrypted devices and is only available as an option when applicable devices are selected.

### Procedure

1. Open **Enterprise Devices** or expand a group and open **Devices**.
   
   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device, then select **Recovery Key**.
   
   The **Recovery Key** screen appears.

   ![Device Recovery Key](image)

3. Copy the recovery key for use on the locked device.
4. Click **OK**.

## Viewing Device Attributes

Use **Device Attributes** to view a current snapshot of the selected device.

### Procedure

1. Open **Enterprise Devices** or expand a group and open **Devices**.
   
   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **Device Attributes**.
   
   The **Device Attributes** screen appears.

## Endpoint Encryption Device Attributes

The following table describes the Endpoint Encryption device attributes.

<table>
<thead>
<tr>
<th>ATTRIBUTE NAME</th>
<th>EXAMPLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Version</td>
<td>2.0.50727.3620</td>
<td>The version and build number for the installed .NET framework</td>
</tr>
<tr>
<td>Common Framework Build Number</td>
<td>5.0.0.84</td>
<td>The Endpoint Encryption agent uses a common framework for encryption. The build number is used to tell whether the agent is up-to-date</td>
</tr>
<tr>
<td>Disk Model</td>
<td>VMware Virtual IDE</td>
<td>The hard disk mode</td>
</tr>
<tr>
<td>Disk Name</td>
<td>\.\PHYSICALDRIVE0</td>
<td>The name of the hard disk</td>
</tr>
<tr>
<td><strong>ATTRIBUTE NAME</strong></td>
<td><strong>EXAMPLE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disk Partitions</td>
<td>1</td>
<td>The number of partitions on the disk with the agent installle.</td>
</tr>
<tr>
<td>Disk Size</td>
<td>10733990400</td>
<td>The total capacity of the hard disk (bytes.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>WORKGROUP</td>
<td>The domain that the endpoint is a membe.</td>
</tr>
<tr>
<td>Endpoint ID</td>
<td>85b1e3e2a3c25d882540ef6e4818c3e4</td>
<td>The unique ID of the endpoint used for Control Manager integration.</td>
</tr>
<tr>
<td>&lt;Agent&gt; User</td>
<td>maryjane</td>
<td>The user name for the last logged on use.</td>
</tr>
<tr>
<td>&lt;Agent&gt; Version</td>
<td>5.0.0.260</td>
<td>The version and build number for the agent installation.</td>
</tr>
<tr>
<td>Hostname</td>
<td>TREND-4136D2DB3</td>
<td>The endpoint's host name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.152.219</td>
<td>The endpoint's IP address.</td>
</tr>
<tr>
<td>Locale</td>
<td>English (United States)</td>
<td>The language and region that the endpoint is configure.</td>
</tr>
<tr>
<td>Machine Name</td>
<td>TREND-4136D2DB3</td>
<td>The computer name that the endpoint use.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>VMware, Inc.</td>
<td>The manufacturer of the hard dis.</td>
</tr>
<tr>
<td>Model</td>
<td>VMware Virtual Platform</td>
<td>The model of the hard dis.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows NT 5.1.2600 Service Pack 3</td>
<td>The operating system installed on the same hard disk as the agent.</td>
</tr>
<tr>
<td><strong>ATTRIBUTE NAME</strong></td>
<td><strong>EXAMPLE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System Name</td>
<td>Microsoft Windows XP Professional</td>
<td>The common name of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Operating System Service Pack</td>
<td>Service Pack 3</td>
<td>The service pack number of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Operating System Version</td>
<td>5.1.2600.196608</td>
<td>The version number of the operating system installed on the same hard disk as the agent</td>
</tr>
<tr>
<td>Partition Scheme</td>
<td>Classical MBR</td>
<td>The partition scheme for the hard disk</td>
</tr>
<tr>
<td>Processor</td>
<td>x86 Family 6 Model 30 Stepping 5, Genuine Intel</td>
<td>The processor make and model of the endpoint</td>
</tr>
<tr>
<td>Processor Count</td>
<td>2</td>
<td>The number of processors in the endpoint</td>
</tr>
<tr>
<td>Processor Revision</td>
<td>1e05</td>
<td>The processor revision number</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Taipei Standard Time</td>
<td>The time zone that the endpoint resides</td>
</tr>
<tr>
<td>Total Physical Memory</td>
<td>2047MB</td>
<td>The total RAM installed in or allocated to the endpoint</td>
</tr>
<tr>
<td>Type</td>
<td>X86-based PC</td>
<td>The endpoint processor type</td>
</tr>
<tr>
<td>Windows User Name</td>
<td>TREND-4136D2DB3\admin</td>
<td>The user name of the Windows account that last logged on the endpoint</td>
</tr>
</tbody>
</table>
Viewing Directory Listing

Note
Use Directory Listing to view the directory structure of KeyArmor devices. Directory Listing is only available in environments that have upgraded from a previous PolicyServer version that had registered KeyArmor devices.

Procedure
1. Open Enterprise Devices or expand a group and open Devices.
   All devices in the Enterprise or group appear in the right pane.
2. In the right pane, right-click the device and select Directory Listing.
   The Device Directory Snapshot screen appears.

Viewing Group Membership

Note
A device can belong to only one group.

Procedure
1. Open Enterprise Devices or expand a group and open Devices.
   All devices in the Enterprise or group appear in the right pane.
2. In the right pane, right-click the device and select List Groups.
   The Group Membership screen appears.
Killing a Device

Initiating a “kill” command deletes all Endpoint Encryption device data. The deleted data is different depending on the scope of data that the associated Endpoint Encryption agent manages. For example, initiating a “kill” command to a Full Disk Encryption device deletes all data from the endpoint, while initiating a “kill” command to a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent. The “kill” command is issued when the Endpoint Encryption agent communicates with PolicyServer.

**WARNING!**
Killing a device cannot be undone. Back up all the data before initiating a kill command.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **Kill Device**.

3. At the warning message, click **Yes**.

4. At the confirmation message, click **OK**.

Locking a Device

Initiating a “lock” command to the Endpoint Encryption device prevents Endpoint Encryption user access until after performing a successful Remote Help authentication. Locking a device reboots the endpoint and forces it into a state that requires Remote Help. The lock command is issued when the Endpoint Encryption agent communicates with PolicyServer.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.
All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the Endpoint Encryption device and select **Lock Device**.

3. At the warning message, click **Yes**.

4. At the confirmation message, click **OK**.

---

**Resetting a Device**

Initiating a “soft reset” command reboots the endpoint. The command issues the next time that the agent communicates with PolicyServer.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the Endpoint Encryption device and select **Soft Reset**.

3. At the warning message, click **Yes**.

4. At the confirmation message, click **OK**.

---

**Restoring a Deleted Device**

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption device.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.

3. Expand the **Recycle Bin**.

4. Open **Deleted Devices**.
   
   The right pane loads all deleted Endpoint Encryption devices.

5. Right-click the Endpoint Encryption device and select **Restore Device**.
   
   The Endpoint Encryption device is added back to the Enterprise, but does not belong to any policy groups.
Part IV

Endpoint Encryption Agent Management
File Encryption

File Encryption protects individual files and folders on local hard drives, and removable media (USB drives). You can set policies specifying which folders and drives are encrypted on the device and policies about encrypted data on removable media. Encryption is performed after authentication takes place.

File Encryption can also protect different files with different keys, allowing you to set access policies to the File Encryption device and separate policies for access to certain files. This is useful in environments where multiple users access one endpoint.

Topics include:

• About File Encryption on page 13-2
• File Encryption Authentication on page 13-2
• File Encryption Agent Menu on page 13-10
• File Encryption Context Menu on page 13-13
• File Encryption Archive Encryption on page 13-14
• File Encryption Archive and Burn on page 13-18
• Using File Encryption Secure Delete on page 13-19
About File Encryption

The Trend Micro File Encryption agent uses AES encryption to protect data that is shared between Endpoint Encryption users, stored on removable media, or saved on network resources. File Encryption can also protect different files with different keys, allowing you to set access policies to the File Encryption agent and then create separate policies for access to certain files, which is useful in environments where multiple users access the same endpoint. Encryption is performed after authentication takes place.

You can use Trend Micro PolicyServer to specify which files and folders are encrypted and policies about encrypting removable media.

End users also have the flexibility to locally manage File Encryption by encrypting individual files, folders, or removable media on the fly, safeguarding their data regardless of where it travels.

File Encryption Authentication

This section explains how to authenticate to and use File Encryption. All authentication methods for Endpoint Encryption are available in File Encryption.

Note
For information about authentication methods, see Authentication Methods on page 2-6.

File Encryption First-time Authentication

When File Encryption is launched for the first time, an initial registration is required to identify PolicyServer. The fixed password authentication method is default. Other options are available depending on policy settings.

Procedure

1. Right-click the File Encryption tray icon, and then select Register.
2. Specify the Endpoint Encryption user name and password.
3. Specify the PolicyServer IP address (or host name) and the Enterprise.

4. Click **OK**.

   The **Change Password** screen appears.

5. Select desired authentication from the drop-down.

6. Specify and confirm the new password, then click **OK**.

   **Note**
   Without authenticating to File Encryption, access to files and removable media is denied.

---

**File Encryption Domain Authentication**

For domain authentication single sign-on (SSO), ensure that the following requirements are met:

- The user belongs to a policy group with domain authentication enabled.
- Make sure that the Host Name and Domain Name are configured properly.
- PolicyServer and all Endpoint Encryption devices using domain authentication are in the same domain.
- The user account is configured in both Active Directory and PolicyServer. The user name is case sensitive and must match exactly.

   **Note**
   For information about configuring domain authentication policies for single sign-on, see *Domain Authentication Policy Rules on page 2-10*. 

---
Authenticating with Domain Authentication

Procedure

1. Use PolicyServer MMC and go to the following policy location:
   
   **File Encryption > Login > Authentication Methods Allowed**

2. Select **Domain Authentication** as the authentication type.

3. Provide the user name and password for the domain account.

4. Click OK.

   **Note**

   • Domain authentication cannot be used with a Smart Card PIN.

   • Remote Help is available to domain users. However, the domain password must be reset in Active Directory if it is forgotten.

File Encryption Smart Card Authentication

To use smart card authentication, make sure that the following requirements are met:

• Enable the File Encryption policy at **Login > Password > Physical Token Required**.

• The smart card reader is connected to the endpoint and the smart card is inserted.

   **Note**

   File Encryption only supports CASC and PIC smart cards

• ActivClient 6.1 with all service packs and updates must be installed.

• Specify the smart card PIN in the password field.
WARNING!
Failure to provide a correct password sends a password error and may result in locking the smart card.

Authenticating with a Smart Card

File Encryption smart card authentication is only available if enabled by policy.

Note
File Encryption only supports CASC and PIC smart cards

Procedure
1. Use PolicyServer MMC and go to the following policy location:
   File Encryption > Login > Authentication Methods Allowed
2. From the Endpoint Encryption device, open File Encryption and select Smart Card from the authentication drop-down.
3. Specify the user name.
4. Specify the smart card PIN or fixed password (if applicable).
5. Click OK.

File Encryption ColorCode Authentication

File Encryption ColorCode authentication is only available if enabled by policy.

Procedure
1. Use PolicyServer MMC and go to the following policy location:
   Group Name > Policies > File Encryption > Login > Authentication Methods Allowed
2. Select ColorCode from the authentication drop-down.
3. Specify the unique ColorCode combination.
4. Click OK.

---

**File Encryption PIN Authentication**

File Encryption PIN authentication is only available if enabled by policy.

**Procedure**

1. Use PolicyServer MMC and go to the following policy location:
   
   Group Name > Policies > File Encryption > Login > Authentication Methods Allowed

2. Select PIN from the authentication drop-down.
3. Specify the PIN combination.
4. Click OK.

---

**Changing Password in File Encryption**

To change the password, the user must authenticate to File Encryption with a User account role. The user can then change the password using any authentication method allowed by policy.

Use PolicyServer MMC to manage the policy at:

Group Name > Policies > File Encryption > Login > Authentication Methods Allowed

**Procedure**

1. Right-click the File Encryption tray icon, then select Change Password.
2. Specify the password.
3. Click Next.
4. Select any available authentication method.
5. Specify and confirm the new password.
6. Click OK.

The new password is updated and a confirmation message appears.

---

**Forced Password Reset**

File Encryption prevents unauthorized access to encrypted files and folders by locking protected files when there are too many unsuccessful authentication attempts or if the endpoint has not communicated with PolicyServer for a specified duration of time. Depending on the policy configuration, File Encryption locks a user from access or enacts a time delay before authentication attempts can be made.

**Using Remote Help to Unlock a File Encryption Device**

If a user exceeds the number of authentication attempts and policies are set to enact Remote Authentication, File Encryption locks Endpoint Encryption folders and notifies the user that Remote Help is required. Using Remote Help to unlock File Encryption requires assistance from the Enterprise Authenticator or Group Authenticator.

---

**Note**

For information about using Remote Help, see Remote Help on page 2-11.

---

**Procedure**

1. Right-click the File Encryption tray icon, then select Remote Help.
The **Remote Help** screen appears.

![Remote Help Screen](image)

**Figure 13-1. File Encryption Remote Help**

2. Specify the user name.
3. Click **Get Challenge**.
4. Type the **Response** provided by the Enterprise/Group Authenticator.
5. Click **Log In**.

   The user is authenticated to File Encryption and a notification displays.

### Endpoint Encryption Device Policy Rules

The following table explains the security policy rules for lost or stolen Endpoint Encryption devices. Depending on the policy settings, too many consecutive unsuccessful authentication attempts to the Endpoint Encryption devices delays the
next authentication attempt, locks the Endpoint Encryption device, or erases all data controlled by the associated Endpoint Encryption agent.

**TABLE 13-1. Device Security Options**

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time delay</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer temporarily locks the Endpoint Encryption device and notifies the Endpoint Encryption user that the device is locked. The ability to authenticate or reset the password is disabled during the time delay. The duration of the time delay is determined by policy. Once the time delay has expired, the user is permitted to authenticate.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The Endpoint Encryption user may use Self Help or Remote Help authentication to avoid waiting for the time delay period to expire.</td>
</tr>
<tr>
<td>Remote authentication required</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer locks the Endpoint Encryption device until the Endpoint Encryption user contacts Technical Support for Remote Help authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Remote Help on page 2-11</em>.</td>
</tr>
<tr>
<td>Erase the device</td>
<td>After exceeding the allowed number of failed authentication attempts, PolicyServer erases all data controlled by the associated Endpoint Encryption agent. For example, erasing a Full Disk Encryption device deletes all data from the endpoint, while erasing a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong></td>
</tr>
<tr>
<td></td>
<td>The Endpoint Encryption user cannot recover the erased data.</td>
</tr>
</tbody>
</table>
File Encryption Agent Menu

Use the File Encryption icon ( ) in the system tray to access to the File Encryption agent. Right-click the agent icon to display the menu items. The following table explains the available menu options.

**Table 13-2. File Encryption Agent Menu Options**

<table>
<thead>
<tr>
<th><strong>Menu Item</strong></th>
<th><strong>Function</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Register</td>
<td>First-time user registration of File Encryption with the PolicyServer. For more information, see <em>File Encryption First-time Authentication on page 13-2.</em></td>
</tr>
<tr>
<td>Log In / Log Out</td>
<td>Authenticate with PolicyServer.</td>
</tr>
<tr>
<td>Change Password</td>
<td>Permits users to change their password. For more information, see <em>Changing Password in File Encryption on page 13-6.</em></td>
</tr>
<tr>
<td>Remote Help</td>
<td>Unlock File Encryption using Remote Help to authenticate if the user forgets the Endpoint Encryption password, there were too many unsuccessful authentication attempts, or the Endpoint Encryption device has not communicated with the PolicyServer for a specified duration. For more information, see <em>Forced Password Reset on page 13-7.</em></td>
</tr>
<tr>
<td>Sync with PolicyServer</td>
<td>Manually download policy updates from PolicyServer. For more information, see <em>Synchronizing Policies with PolicyServer on page 13-11.</em></td>
</tr>
<tr>
<td>Sync with PolicyServer</td>
<td>Synchronizing with PolicyServer offline files enforces new security policies using an import file instead of communicating directly with PolicyServer. For more information, see <em>Synchronizing Policies with PolicyServer Offline Files on page 13-12.</em></td>
</tr>
<tr>
<td>Offline Files</td>
<td></td>
</tr>
<tr>
<td>Hide Notification</td>
<td>Silences all File Encryption notifications.</td>
</tr>
<tr>
<td>About File Encryption</td>
<td>Displays File Encryption information including version, last sync time, and authenticated user.</td>
</tr>
<tr>
<td>Close Tray</td>
<td>Temporarily removes the File Encryption tray icon.</td>
</tr>
</tbody>
</table>
Synchronizing Policies with PolicyServer

File Encryption agents can manually download new policies by opening the File Encryption tray icon and selecting **Sync with PolicyServer**.

---

**Note**

File Encryption agents can synchronize policies without user authentication.

If a network connection or PolicyServer is unavailable, a **Failed to sync with server** error display.

---

Automatic Policy Synchronization

The following list explains the events that initiate policy synchronization between all Endpoint Encryption agents and PolicyServer.

- After the operating system loads and the Endpoint Encryption agent service starts

---

**Note**

For information about Endpoint Encryption services, see *Endpoint Encryption Services on page C-1*.

---

- When the Full Disk Encryption preboot starts (Full Disk Encryption only)
- The time duration of the **Sync Interval** policy elapses

Open the **About** screen in the Endpoint Encryption agent to manually synchronize policies.

---

**Note**

Endpoint Encryption device actions initiate after the Endpoint Encryption agent receives policy updates.
Synchronizing Policies with PolicyServer Offline Files

Offline updates work with the File Encryption 3.0.13.2447 or higher and now work on x64 installs of File Encryption. If the update is generated, the offline update replaces any existing user password with the new fixed password.

Synchronized passwords will not replace a user password on update to maintain the same functionality of managed devices.

A fixed password is required to add a user to an offline File Encryption device. The offline process will generate two files:

Changing PolicyServer

Use the File Encryption About menu to update the PolicyServer that manages policies.

Procedure

1. Right-click the File Encryption tray icon, then select About File Encryption.
   
   The About windows appears.

2. Click Edit PolicyServer.

3. Specify the new PolicyServer host name or IP address.

4. Click OK.

   File Encryption is now managed by the new PolicyServer.
File Encryption Context Menu

Users can encrypt a file by right-clicking the file and selecting an encryption option. The following illustration shows some of the options available.

![File Encryption Context Menu](image)

**Figure 13-2. File Encryption Context Menu**

Use the following table to understand the available menu options.

**Table 13-3. File Encryption Context Menu Options**

<table>
<thead>
<tr>
<th><strong>Menu Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>Create an encrypted copy of the specified file.</td>
</tr>
<tr>
<td>Expand Archive</td>
<td>Open a previously created archive.</td>
</tr>
<tr>
<td>Archive and Burn</td>
<td>Create an encrypted copy of the specified file and write it to CD/DVD.</td>
</tr>
<tr>
<td>Secure Delete</td>
<td>Securely erase the selected files and the file history from the File Encryption device.</td>
</tr>
</tbody>
</table>
File Encryption Archive Encryption

File Encryption encrypts files based on policies defined locally or policies defined by PolicyServer. The encryption method depends on user needs for file access and the level of security desired.

To automatically encrypt files, save them in the following locations:

• A folder on the File Encryption device
• A folder that resides on removable media
• A fully encrypted removable media device

File Encryption Local Key Encryption

Selecting the Local Key function allows a user to encrypt files for view strictly by that user. Local Key files can only be accessed on a File Encryption device by the user who created them.

The policies are available at:

• In Control Manager, go to Policies > Policy Management, select the policy, then modify Common policy rules. For more information, see Configuring Common Policy Rules on page 3-19.

• PolicyServer MMC, set File Encryption > Encryption > Encryption Method Allowed to User's Unique Key

Note

File Encryption creates a new file when encrypting a file. The original file remains unencrypted in its original location.
WARNING!

Depending on the Windows operating system, a user may view folder contents if switching from one user to a separate user without restarting Windows. While file names and folder content may be viewed, the file contents are not available. This is due to Windows operating system caching the file structure for quick search capability.

Creating a Local Key

Procedure

- Right-click the desired file, then go to File Encryption > Archive > Local Key.

  The original files or folders are unchanged and can be kept or deleted.

File Encryption Shared Key Encryption

Use the Shared Key function to encrypt files strictly for access by members of the same policy group.

The policies are available at:

- In Control Manager, go to Policies > Policy Management, select the policy, then modify Common policy rules. For more information, see Configuring Common Policy Rules on page 3-19.

- PolicyServer MMC, set File Encryption > Encryption > Encryption Method Allowed to Group Key

  **Note**
  
  To allow any File Encryption user within the PolicyServer Enterprise, to view encrypted files, set Encryption Key Used to Enterprise Key.

  **Note**
  
  File Encryption creates a new file when encrypting a file. The original file remains unencrypted in its original location.
**WARNING!**

Depending on how Windows permissions are configured, a user can view encrypted folder contents if switching between users without restarting Windows. While the file names and folder content may be viewed, the file contents are not available. This is due to Windows Operating system caching the file structure for quick search capability.

---

**Creating a Shared Key**

**Procedure**

- Right-click the desired file, then go to **File Encryption > Archive > Shared Key**.

  The original files or folders are unchanged to keep or delete.

---

**File Encryption Fixed Password Encryption**

File Encryption can create encrypted files using a fixed password. Users can optionally set the file to self-extract so that the recipient does not need File Encryption to decrypt the file.

**Note**

- There is no functionality available for password recovery with self-extracting files. If a password is forgotten, the encrypted file cannot be recovered.
- Due to a Windows limitation, executable (self-extracting) files cannot be larger than 2GB.

---

**Creating a Fixed Password Key**

**Procedure**

1. Right-click the desired file, then go to **File Encryption > Archive > Fixed Password**.

2. Specify and confirm the fixed password.
3. Optionally select **Output encrypted data as a self-extracting archive**, if necessary.

4. Click **OK**.
   
The file encrypts.

5. To decrypt the file, do the following:
   a. Double-click the file.
   b. Specify the archive password.
   c. Click **OK**.

6. For self-extracting archives, do the following:
   a. Double-click the file.
   b. Specify the archive password.
   c. Select the extraction location.
   d. Select whether to open destination after extraction or to overwrite existing files.
   e. Click **Continue**.

   The original files or folders are unchanged and can be kept or deleted.

---

**File Encryption Digital Certificate Encryption**

File Encryption can encrypt files with digital certificates (smart cards) from the Windows certificate store.

**Creating a Digital Certificate Key**

**Procedure**

1. Right-click the desired file, then go to **File Encryption > Archive > Certificate**.
2. Select a **Certificate Store**.

3. Click **Gather Certificates**.

4. Select one or more certificates, then click **OK**.

---

**Note**

Certificates are gathered from the Windows certificate store.

---

5. Insert a blank CD/DVD inserted in an available optical drive.

6. Select the optical drive.

7. Click **OK**.

   The original files or folders are unchanged and can be kept or deleted.

---

**File Encryption Archive and Burn**

The File Encryption Use the **Archive and Burn** function to write encrypted files to a CD or DVD. Files are self-extracting and can encrypt using a fixed password or digital certificate.

**Burning an Archive with a Fixed Password**

**Procedure**

1. Right-click the file, then go to **File Encryption > Archive and Burn > Fixed Password**.

2. Specify and confirm the password.

3. Insert a burnable disk into the CD/DVD optical drive.

4. Select the optical drive.

5. Click **OK**.
The self-extracting file is burned to CD/DVD.

**Burning an Archive with a Certificate**

**Procedure**

1. Right-click the file, then go to **File Encryption > Archive and Burn > Certificate** from the File Encryption context menu.
2. Select a **Certificate Store**.
3. Click **Gather Certificates**.
4. Select one or more certificates, then click **OK**.
5. Select an optical drive with a black CD/DVD inserted.
6. Click **OK**.

The self-extracting file is burned to CD/DVD.

**File Encryption Secure Delete**

Use Secure Delete to securely erase the selected files and the file history from the File Encryption device.

**Using File Encryption Secure Delete**

**Procedure**

1. Right-click the file and go to **File Encryption > Secure Delete**.
2. Click **Yes** to permanently delete the file.
Chapter 14

Full Disk Encryption

Full Disk Encryption provides comprehensive endpoint data security using mandatory strong authentication and full disk encryption. Full Disk Encryption secures not only the data files, but also all applications, registry settings, temporary files, swap files, print spoolers, and deleted files. Until the user is validated, strong preboot authentication restricts access to the vulnerable host operating system.

Topics include:

• About Full Disk Encryption on page 14-2
• Endpoint Encryption Tools on page 14-2
• Full Disk Encryption Preboot on page 14-3
• Full Disk Encryption Connectivity on page 14-17
• Full Disk Encryption Recovery Console on page 14-20
• Full Disk Encryption Recovery Methods on page 14-32
• Repair CD on page 14-34
• Patch Management with Full Disk Encryption on page 14-41
About Full Disk Encryption

The Trend Micro Full Disk Encryption agent combines a robust AES256 encryption algorithm and mandatory authentication to make data inaccessible without authentication. Full Disk Encryption prevents data loss by encrypting the whole drive, including operating system, program, temporary, and end user files.

Full Disk Encryption allows for the flexibility to use either software-based encrypted hard drives or hardware-based encrypted hard drives as needed. Seagate DriveTrust™, OPAL, and OPAL2 self-encrypting drives are supported. While hardware-based encryption is simpler to deploy on new hardware, easier to maintain, and offers a higher level of performance, software-based encryption does not require any hardware and is cheaper to deploy to existing endpoints.

Trend Micro PolicyServer controls policies affecting Full Disk Encryption, ensuring complete endpoint security centrally managed across the Enterprise. Full Disk Encryption is network-aware and updates policies before allowing authentication. You can also remotely lock or wipe data on the endpoint before the operating system or any other sensitive data is accessed.

Trend Micro Endpoint Encryption 5.0 advances Full Disk Encryption by integrating with encryption solutions built into the host operating system through two new Endpoint Encryption agents:

• Encryption Management for Microsoft BitLocker
• Encryption Management for Apple FileVault

Endpoint Encryption Tools

The following table describes the various tools available for Endpoint Encryption.
### Table 14-1. Endpoint Encryption Tools

<table>
<thead>
<tr>
<th>TOOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Console</td>
<td>Use Recovery Console to recover from an operating system critical error, troubleshoot network issues, and manage users or logs.</td>
</tr>
<tr>
<td>Command Line Helper</td>
<td>Use Command Line Helper to create encrypted values to secure credentials when creating an installation script.</td>
</tr>
<tr>
<td>Command Line Installer Helper</td>
<td>Use Command Line Installer Helper to generate scripts for automated installations and to create encrypted values for credentials when creating the scripts.</td>
</tr>
<tr>
<td>DAAutoLogin</td>
<td>Use DAAutoLogin for Windows patching. DAAutoLogin allows for a one-time bypass of Endpoint Encryption Preboot.</td>
</tr>
<tr>
<td>Repair CD</td>
<td>Use the bootable Repair CD to decrypt the hard disk before removing Full Disk Encryption in the event that the disk becomes corrupted. Only use the Repair CD if standard removal methods are not possible. A typical symptom of a corrupted disk is a black screen.</td>
</tr>
</tbody>
</table>

### Full Disk Encryption Preboot

After installing Full Disk Encryption, the Full Disk Encryption preboot appears before Windows loads. The Full Disk Encryption preboot ensures that only authorized users are able to access endpoints and updates local security policies when connected to PolicyServer.

---

**Note**

Use PolicyServer MMC to optionally make the user name case sensitive.
FIGURE 14-1. The Full Disk Encryption Preboot Screen

Menu Options

There are several options available in the upper-left menu of Full Disk Encryption Preboot.

TABLE 14-2. Full Disk Encryption Preboot Menu Options

<table>
<thead>
<tr>
<th>MENU ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Change the authentication method used to log on to Endpoint Encryption devices.</td>
</tr>
<tr>
<td>Communication</td>
<td>Manually synchronize with PolicyServer.</td>
</tr>
</tbody>
</table>

**Note**
The Communication menu item is not available for unmanaged endpoints.
Network Connectivity

The network connection icon (.internet) appears in the upper-right corner when Full Disk Encryption is installed as a managed endpoint. The icon is only highlighted when the device is connected to the network and has communication with PolicyServer. When Full Disk Encryption is unmanaged, the network icon never displays.

Connecting to a Wireless Network

The wireless connection icon (wireless) appears in the upper-right corner of the Full Disk Encryption preboot logon when the endpoint has a detected wireless card installed. If there is no wireless card detected, the wireless network icon does not display.

**Note**

The Full Disk Encryption preboot cannot automatically detect the authentication for WEP security. If the authentication type is WEP-OPEN or WEP-PSK, manually specify the security type.

**Procedure**

1. Click the wireless icon in the upper-right corner of the Full Disk Encryption preboot logon.
The **Access Connection** screen appears.

![Access Connection Screen](image)

2. Click **All Access Points**.
The Wireless Network Configuration screen appears.

3. Do one of the following:
   - To use a listed network, select the SSID, then click OK.
   - To configure an unlisted network, click Other Network, specify the SSID settings, then click Connect.

4. Wait for Full Disk Encryption to configure wireless access.

5. Click Close to complete the wireless network setup.

---

On-Screen Keyboard

Access the on-screen keyboard from Full Disk Encryption preboot by going to Menu > Computer > On-Screen Keyboard.
To insert the cursor in the desired field when the keyboard is displayed, click Focus on the bottom-right corner of the keyboard.

### Changing the Keyboard Layout

Changing the keyboard layout affects both keystrokes and the on-screen keyboard. Once Windows boots, the keyboard layout is set by the Windows operating system. A restart is required to commit the keyboard layout changes.

**Procedure**

1. Go to **Menu > Computer > Change Keyboard Layout**.
   
   The **Select the keyboard language (layout)** window appears.

2. Select a keyboard layout.

3. Click **OK**.

4. Click **OK** to restart the endpoint.

### Changing Authentication Methods

**Note**

For information about authentication methods, see Authentication Methods on page 2-6.

**Procedure**

1. From the Full Disk Encryption preboot, select **Change Password After Login**.

2. Specify the user name and password.

3. Click **Login**.
The Change Password window appears. The interface is different for different authentication methods.

**FIGURE 14-2. Example Of Changing A Fixed Password**

4. From the upper-left menu, select Authentication, then select the desired authentication method.

   The New Password window for the chosen authentication method appears.

5. Provide and confirm the new password, and then click Next.

   The device boots into Windows.

**Changing Passwords**

The following procedure explains how to change the Endpoint Encryption user account password using the Full Disk Encryption preboot.
Procedure

1. Specify the Endpoint Encryption user name and password.

2. Select **Change Password After Login**.

3. Click **Login**.

   The **Change Password** window appears. The interface is different for different authentication methods.

   ![Change Password Window](image)

   **Figure 14-3. Changing A Fixed Password Screen**

4. Provide and confirm the new password, and click **Next**.

   The device boots into Windows.

ColorCode

ColorCode™ is a unique authentication method designed for quick access and easy memorization. Rather than alphanumeric characters or symbols for the password,
ColorCode authentication consists of a user-created color sequence (example: red, red, blue, yellow, blue, green).

![ColorCode Authentication Screen](image)

**Figure 14-4. ColorCode Authentication Screen**

**Creating a ColorCode Password**

The total number of steps in the ColorCode (count) is defined by PolicyServer. The default count is six.

**Procedure**

1. Start the endpoint and wait for the Full Disk Encryption preboot to appear.
2. Follow the instructions to change passwords.
   
   See *Changing Passwords on page 14-9*.
3. Change the authentication method to ColorCode.
Note

For information about changing authentication methods, see Changing Authentication Methods on page 14-8.

The ColorCode Change Password screen appears.

![ColorCode Change Password Screen](image)

**Figure 14-5. ColorCode Change Password Screen**

4. Select the first color by clicking it using the square to the left.
   
The count increases by one.

5. Click additional colors in the sequence.

   **Tip**

   Click Back to change the last color clicked, or click Clear to start over.

6. After the sequence is complete, confirm the ColorCode password using the square to the right.

7. Click Next to finish.
Remote Help

Remote Help allows Group or Enterprise Authenticators to assist Endpoint Encryption users who are locked out and cannot log on to Endpoint Encryption devices after too many unsuccessful log on attempts, or when the period between the last PolicyServer synchronization has been too long.

Using Remote Help to Unlock Full Disk Encryption Devices

**Important**
- Restarting the Endpoint Encryption device resets the challenge code.
- Manually synchronizing policies with PolicyServer also resets the challenge code.
- The challenge code and response code are not case sensitive.

**Procedure**

1. From the Full Disk Encryption preboot, go to **Menu > Authentication > Remote Help**.
2. Provide the **Challenge Code** to the Policy/Group Administrator.
3. Specify the **Response Code** provided by the Policy/Group Administrator.
4. Click **Login**.
   The **Change Password** screen appears.

**Note**

If the account uses domain authentication, the endpoint boots directly into Windows.

5. Specify and confirm new password, then click **Next**.
   The device boots into Windows.
Smart Card

Smart card authentication requires both a PIN and a physical token to confirm the user identity. To use smart card authentication, make sure that the following requirements are met:

• The smart card reader is connected to the endpoint and the smart card is inserted into the smart card reader.
• ActivClient 6.1 with all service packs and updates are installed.
• Specify the smart card PIN in the password field.

**WARNING!**

Failure to provide a correct password sends a password error and may result in locking the smart card.

---

**Note**

Smart card authentication is only configurable with PolicyServer MMC.

Enable smart card authentication for each Endpoint Encryption agent:

• For File Encryption, go to Login > Password > Physical Token Required.
• For Full Disk Encryption, go to Full Disk Encryption > Login > Token Authentication

**Smart Card Registration**

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

Use one of the following methods to register a smart card:

• To use the Full Disk Encryption preboot, see Registering a Smart Card in Full Disk Encryption Preboot on page 11-25.
• To use PolicyServer MMC, see *Configuring Smart Card Authentication in PolicyServer MMC* on page 11-24.

**Registering a Smart Card in Full Disk Encryption Preboot**

**Procedure**

1. Follow the instructions to change passwords, then select **Smart Card**.
   
   See *Resetting User Passwords* on page 11-21.

2. Insert the smart card in the reader.

3. Connect the reader to the endpoint.

4. Specify the user name and fixed password.

5. Click **Continue**.

6. At the confirmation message, click **Continue**.

7. At the **Register Token** window, do the following:
   
   a. Type the new PIN provided by the Group or Enterprise Administrator.
   
   b. Confirm the new PIN.
   
   c. Select the smart card type from the **Token** drop-down list.
   
   d. Click **Continue** to finish registering the smart card token.

**Self Help**

Self Help authentication allows Endpoint Encryption users who have forgotten the credentials to answer security questions and log on to Endpoint Encryption devices without getting Technical Support assistance. Self Help is not available to Enterprise or Group Administrator and Authenticator accounts. Self Help requires the Endpoint Encryption user to respond with answers to predefined personal challenge questions. Self Help can replace fixed password or other authentication methods.
Note
Self Help is only configurable with PolicyServer MMC.

Make sure to allow Self Help authentication. For more information, see Authentication Policies on page 9-30.

WARNING!
Self Help can have a maximum of six questions. Do not create more than six questions or users cannot log on using Self Help authentication.

Setting Up Self Help

If the Self Help policy is enabled, the user is prompted to define answers for the Self Help questions after his/her first login. If the user changes their password, they must define Self Help question answers again.

Note
Self Help answers are stored on the device. If a user logs on another Full Disk Encryption device, the user must define Self Help answers for that device.

Procedure

1. Provide the user name and password.
2. Click Login.
   The Self Help window appears.
3. Define answers for all of the Self Help questions.
4. Click Next.
   The device boots into Windows.
Using Self Help

Procedure

1. From the top-left menu of Full Disk Encryption Preboot, go to **Menu > Authentication > Self Help**.
   
   The **Self Help** window appears.
2. Answer all of the Self Help questions.
3. Click **Login**.
4. Define a new password, and then click **Next**.
   
   The device boots into Windows.

Changing Self Help Answers

Procedure

1. From the Full Disk Encryption preboot, provide the credentials, select **Change Password After Login**, then click **Login**.
   
   The **Change Password** window appears.
2. Provide and confirm the new password, then click **Next**.
   
   The **Self Help** window appears.
3. Define new answers for all Self Help questions, then click **Next**.
   
   The Endpoint Encryption device boots into Windows.

Full Disk Encryption Connectivity

Endpoint Encryption uses a FIPS 140-2 approved encryption process for data passed between the Full Disk Encryption preboot and PolicyServer. Full Disk Encryption
agents that have network connectivity to PolicyServer can receive policy updates and upload audit data from the agent. All client-server communications are internally encrypted and can be sent over insecure connections such as the Internet.

You can place PolicyServer within a DMZ (Demilitarized Zone) for access to both internal networks and the Internet. For information about different network topology configurations, see the *Endpoint Encryption Installation and Migration Guide*.

**TABLE 14-3. Full Disk Encryption Connectivity Requirements**

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolicyServer</td>
<td>Updated security policies from PolicyServer are sent to the Full Disk Encryption preboot or by connectivity established within Windows, LAN, or VPN.</td>
</tr>
<tr>
<td>TCP/IP Access</td>
<td>Network connectivity requires full TCP/IP network access; dial-up or telephone access cannot be used to provide connectivity with PolicyServer during preboot authentication.</td>
</tr>
<tr>
<td>Port</td>
<td>Endpoint Encryption agents communicate using port 8080 by default. To change the default port number, go to Recovery Console and update the PolicyServer. For details, see <em>Changing the Full Disk Encryption PolicyServer on page 14-23</em>.</td>
</tr>
</tbody>
</table>

**Automatic Policy Synchronization**

The following list explains the events that initiate policy synchronization between all Endpoint Encryption agents and PolicyServer.

- After the operating system loads and the Endpoint Encryption agent service starts

  **Note**

  For information about Endpoint Encryption services, see *Endpoint Encryption Services on page C-1*.

- When the Full Disk Encryption preboot starts (Full Disk Encryption only)
- The time duration of the **Sync Interval** policy elapses
Open the **About** screen in the Endpoint Encryption agent to manually synchronize policies.

---

**Note**

Endpoint Encryption device actions initiate after the Endpoint Encryption agent receives policy updates.

---

### Updating Full Disk Encryption Agents

Full Disk Encryption agents automatically receive policy updates from PolicyServer at intervals determined by policy.

Do either of the following to manually update policies.

---

**Procedure**

- Use the Full Disk Encryption preboot.
  
  a. Go to **Communications** > **Synchronize policies**.
  
  b. Go to **Computer** > **About Full Disk Encryption**.
      
      The timestamp of the latest PolicyServer policy synchronization displays.

- Use the Full Disk Encryption agent.
  
  a. Double-click the Full Disk Encryption icon ( Yorkers ) in the Windows system tray.
      
      The Full Disk Encryption agent opens.
  
  b. Click **Synchronize with PolicyServer**.
      
      After a moment PolicyServer enforces all new policies changes.
Full Disk Encryption Recovery Console

Recovery Console helps you recover Full Disk Encryption devices in the event of primary operating system failure, troubleshoot network connectivity issues, and manage policies when not connected with PolicyServer.

---

**WARNING!**

Use Recovery Console before running standard Windows diagnostic and repair utilities. All policy changes are overwritten when the Full Disk Encryption agent synchronizes policies with PolicyServer.

---

Recovery Console Options

<table>
<thead>
<tr>
<th><strong>Console Menu</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Back to Login</td>
<td>Exit Recovery Console and return to the login screen.</td>
</tr>
<tr>
<td>Decrypt Disk</td>
<td>Remove encryption from the disk drive. Use the Full Disk Encryption Preboot Recovery Console to access Decrypt Disk.</td>
</tr>
<tr>
<td>Mount Partitions</td>
<td>Provide access to the encrypted partitions for file management. Use the Full Disk Encryption Preboot Recovery Console to access Mount Partitions.</td>
</tr>
</tbody>
</table>

**Note**

Mount Partitions is only accessible on devices with software encryption. This option is grayed-out if a device has hardware encryption.
### Console Menu

<table>
<thead>
<tr>
<th><strong>Console Menu</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Boot</td>
<td>Roll back the MBR to a state before Full Disk Encryption installation. Use the Full Disk Encryption Preboot Recovery Console to access Restore Boot.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Restore Boot is only accessible on devices with software encryption. This option is grayed-out if a device has hardware encryption.</td>
</tr>
<tr>
<td>Manage Users</td>
<td>Add or remove users from the device when not connected to PolicyServer.</td>
</tr>
<tr>
<td>Manage Policies</td>
<td>Modify policies for devices that are either not managed by PolicyServer or are managed but are temporarily not connected to PolicyServer. If the device is managed, policy changes are overwritten the next time that the device communicates with PolicyServer.</td>
</tr>
<tr>
<td>View Logs</td>
<td>View and search the various Full Disk Encryption logs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Logs are available only when the Recovery Console is accessed from Windows.</td>
</tr>
<tr>
<td>Network Setup</td>
<td>Verify, test, and modify network settings.</td>
</tr>
<tr>
<td>Exit</td>
<td>Exit the Recovery Console.</td>
</tr>
</tbody>
</table>

### Accessing Recovery Console from Full Disk Encryption Preboot

Only Enterprise or Group Administrator and Authenticator accounts can access Recovery Console.

**Procedure**

1. To allow users to access Recovery Console, enable the following policy:
Full Disk Encryption > Agent > Allow User Recovery

2. Reboot the endpoint.

The Full Disk Encryption preboot appears.

3. Select the **Recovery Console** check box.

4. Specify Endpoint Encryption user account credentials.

5. Click **Login**.

Recovery Console opens.

---

**Accessing Recovery Console from Windows**

**Procedure**

1. In Windows, go to the Full Disk Encryption installation directory.

   The default location is `C:\Program Files\Trend Micro\Full Disk Encryption\`.

2. Open `RecoveryConsole.exe`.

   The **Recovery Console** window appears.

3. Specify the Endpoint Encryption user name and password, then click **Login**.

   Recovery Console opens to the **Decrypt Disk** page.

---

**Full Disk Encryption PolicyServer Settings**

Full Disk Encryption PolicyServer settings are configurable by going to the Recovery Console from the Full Disk Encryption preboot or by running `C:\Program Files\Trend Micro\Full Disk Encryption\RecoveryConsole.exe`. 
Changing the Full Disk Encryption PolicyServer

Note
Changing the PolicyServer requires access to Full Disk Encryption Recovery Console. For more information, see Full Disk Encryption PolicyServer Settings on page 14-22.

Procedure
1. From the Full Disk Encryption Recovery Console, click the PolicyServer tab.
2. Click Change Server.
3. At the warning message, click Yes.
4. Specify the new server address.
5. Click Save.

Using Decrypt Disk

Selecting Decrypt Disk decrypts an encrypted Full Disk Encryption hard disk, but does not remove any of the encryption drivers. If using Decrypt Disk, disable the Full Disk Encryption “DrAService” service before booting into Windows.

WARNING!
Read this procedure before using Decrypt Disk. Data loss may occur if performed incorrectly. Do not use Decrypt Disk to remove Full Disk Encryption from any Endpoint Encryption device that is functioning normally. Use TMFDEUninstall.exe instead.

Procedure
1. Log on to Recovery Console.

See Accessing Recovery Console from Full Disk Encryption Preboot on page 14-21.

Recovery Console opens to the Decrypt Disk page.
2. Click **Decrypt** to begin decrypting the drive. 
   Decryption begins immediately and the **Decrypt Disk** page shows the decryption progress.

3. When decryption completes, click **Exit** to reboot the Endpoint Encryption device.

4. Do one of the following:
   - If booting a repair tool CD, DVD, or USB key:
     a. After exiting Full Disk Encryption, press **F12** (or the appropriate button to enter the boot options).
     b. Insert the Repair CD and select the CD/DVD drive from the boot options screen.
     c. Proceed with established recovery actions.
   - If booting into Windows:
     a. Reboot the endpoint and hold **F8**.
     b. Select **Safe Mode** before the system begins booting into Windows.

   **WARNING!**
   If the Windows boot options screen is missed, immediately turn off the device. 
   If Windows boots normally (not in Safe Mode), DrAService will immediately start encrypting the drive again. Any recovery actions taken at this point will risk irreparable damage to data on the drive.

5. Open **Computer Management** and go to **Services and Applications** > **Services**.
   The **Services** screen appears.

6. Locate and double-click **Trend Micro Full Disk Encryption** to open the **Trend Micro Full Disk Encryption Properties** window.

7. On the **General tab**, change **Startup type** to **Disabled**.

8. Click **Apply**, then click **OK**.
9. Reboot the endpoint.

10. Log on to the Full Disk Encryption preboot.

11. Log on to Windows.

12. After all recovery actions are complete, set DrAService to Automatic. The device automatically re-encrypts the hard disk after the next reboot.

---

### Mount Partitions

Use Mount Partitions to copy files between the encrypted hard disk and external storage before imaging or reformatting the drive. The encrypted contents on the drive appear in the left pane and an unencrypted device can be mounted in the right pane. Use copy and paste to move files between panes. Files copied to the encrypted drive will encrypt. Files copied out of the encrypted drive will decrypt.

### Restore Boot

The Restore Boot option restores the original boot on the Endpoint Encryption device when the device is fully decrypted. Restore Boot is only available from the Full Disk Encryption preboot.

Decrypt the disk before restoring the Master Boot Record (MBR).

---

**WARNING!**

Do not use Decrypt Disk before reading through the instructions. Data loss may occur.

---

### Procedure

1. Log on to Recovery Console.

   See Accessing Recovery Console from Full Disk Encryption Preboot on page 14-21.

   Recovery Console opens to the Decrypt Disk page.

2. Click Decrypt Disk, then click Decrypt.
3. Switch to the **Restore Boot** option.
   
   A **Replace MBR** confirmation window appears.

4. Click **Yes** to replace the MBR.
   
   A message confirming the MBR replacement displays.

5. Click **Exit**.
   
   The Endpoint Encryption device boots into Windows.

---

### Manage Full Disk Encryption Users

Use **Manage Users** to add or remove users from the Full Disk Encryption preboot cache or to change a user's cached password. The **Manage Users** option is useful when the Full Disk Encryption agent cannot connect to PolicyServer. Both the Full Disk Encryption preboot and Windows Recovery Console can use this option.

---

**Note**

- **Manage Users** is only available when not connected to PolicyServer.
- Changes made to users through Recovery Console are overridden when Full Disk Encryption connects to PolicyServer.

---

Some considerations about passwords:

- Assigned passwords are always a fixed password.
- Specify the user password expiration date using the **Password Expiration** calendar.
- Setting the date to the current date or older forces an immediate password change. Setting the date to a future date commits a change on that specified date.

---

### Editing Users

Editing users in Recovery Console follows the same rules as the Enterprise. For information about roles and authentication, see **Devices and Users Overview on page 2-1**.
**Procedure**

1. Select the user from the user list.
2. Update the desired information.
3. Select the user type.
   
   For an explanation of account roles, see *Devices and Users Overview on page 2-1*.
4. Set the password expiration date.
5. Click **Save**.
   
   The user account is updated.

---

**Adding Users**

**Procedure**

1. Click **Add User**.
2. Specify the user name and password, then confirm the password.
3. Select the authentication method from the **Authentication Type** drop-down list.
4. Set the password expiration date.
5. Click **Save**.
   
   The new user appears in the User List and a confirmation window appears.
6. Click **OK** to close the confirmation window.
   
   The new user account is added.
Deleting Users

Procedure

1. Select a user from the user list.
2. Click **Delete User**.
   A delete user confirmation window appears.
3. Click **Yes**.
   The user is deleted from the user list.

Manage Policies

Use **Manage Policies** to set various policies for Full Disk Encryption Recovery Console. For an explanation of these policies, see *Policies in PolicyServer MMC on page 9-1*.

**Note**

The **Manage Policies** option is only available when not connected to PolicyServer and any changes are overridden the next time Full Disk Encryption connects to PolicyServer.

View Logs

Use **View Logs** to search for and display logs based on specific criteria. **View Logs** is only available from Recovery Console using Windows. It is unavailable from the Full Disk Encryption Preboot.

For information about viewing Full Disk Encryption logs, see *Accessing Recovery Console from Windows on page 14-22*.
Network Setup

Use Network Setup to verify, test, and/or change the network settings that are used by Full Disk Encryption Preboot. There are three tabs: IPv4, IPv6, and PolicyServer.

Managing Network Configuration

By default, Get setting from Windows is selected for both IPv4 and IPv6. Deselect this option to manually configure the network settings.

- Selecting DHCP (IPv4) or Automatically get address (IPv6) uses the dynamically assigned IP address.
- Selecting Static IP enables all fields in that section.
- In the IPv6 tab, selecting Static IP when the IP Address field is empty creates a unique IP address based on the hardware address of the machine.

Migrating Full Disk Encryption to a New Enterprise

One PolicyServer instance may have multiple Enterprise configurations that each represent a business unit or department. Moving to a new Enterprise removes the Endpoint Encryption device from the old Enterprise and adds the Endpoint Encryption device to the new Enterprise within the same PolicyServer instance. The Full Disk Encryption agent may need to move to a new Enterprise when the employee moves to a different department or office location.

Note

For information about changing the PolicyServer that manages the Full Disk Encryption agent, see Changing the Full Disk Encryption PolicyServer on page 14-23.

Changing the Enterprise requires access to Full Disk Encryption Recovery Console. For more information, see Full Disk Encryption PolicyServer Settings on page 14-22.

WARNING!

Changing the Enterprise requires configuring policies again, recreating groups, and deletes all cached passwords, password history, and audit logs.
Procedure

1. Click Network Setup.

2. Select the PolicyServer tab.

3. Click Change Enterprise.

   The Change Enterprise screen appears.

   ![](image)

   **Figure 14-6. Recovery Console Change Enterprise**

4. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Server User</td>
<td>Specify an Enterprise Administrator account user name, or the user name of an account with permission to install to the Enterprise or group in the new PolicyServer.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New User Password</td>
<td>Specify the password for the Enterprise Administrator account.</td>
</tr>
<tr>
<td>New Server Address</td>
<td>Specify the new PolicyServer IP address or host name.</td>
</tr>
<tr>
<td>New Enterprise</td>
<td>Specify the new PolicyServer Enterprise.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
   
   Full Disk Encryption validates the new PolicyServer information.

6. At the confirmation message, click **OK**.

---

### Changing the Full Disk Encryption PolicyServer

**Note**

Changing the PolicyServer requires access to Full Disk Encryption Recovery Console. For more information, see *Full Disk Encryption PolicyServer Settings on page 14-22*.

---

**Procedure**

1. From the Full Disk Encryption Recovery Console, click the **PolicyServer** tab.

2. Click **Change Server**.

3. At the warning message, click **Yes**.

4. Specify the new server address.

5. Click **Save**.
Full Disk Encryption Recovery Methods

Once a Full Disk Encryption device is fully encrypted, scenarios may exist where you must perform system restore actions, such as a lost Local Administrator password or a corrupted Windows environment.

---

**Important**

Decrypt the drive before performing recovery actions. For software encryption, standard data recovery tools (Windows Recovery Disk, ERD Commander, UBCD) cannot access a Full Disk Encryption 5.0 or higher encrypted device.

---

Data recovery methods are available to Endpoint Encryption Administrator and Authenticator accounts to recover data when the Full Disk Encryption device is not properly functioning.

---

**Note**

To decrypt the Full Disk Encryption device, the user must have Endpoint Encryption Enterprise or Group Administrator rights. To allow all users in a group/policy to access the recovery console, enable the following policy:

<table>
<thead>
<tr>
<th>MANAGEMENT CONSOLE</th>
<th>MENU PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolicyServer MMC</td>
<td>Go to <strong>Full Disk Encryption &gt; Agent &gt; Allow User Recovery.</strong></td>
</tr>
<tr>
<td>Control Manager</td>
<td>Create or edit a policy, then go to <strong>Full Disk Encryption &gt; Users are allowed to access system recovery utilities.</strong></td>
</tr>
</tbody>
</table>
## Recovery Methods for Full Disk Encryption-protected devices

<table>
<thead>
<tr>
<th>Recovery Method</th>
<th>Description</th>
<th>Usage Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption Uninstall</td>
<td>Full Disk Encryption Uninstall removes Full Disk Encryption from the device. Once the uninstall is complete, you may proceed with established recovery action within Windows.</td>
<td>Windows environment is working normally.</td>
</tr>
<tr>
<td>Recovery Console</td>
<td>Selecting the Full Disk Encryption <strong>Recovery Console &gt; Decrypt Disk</strong> option decrypts the selected hard disk on-the-fly or saves an image of the decrypted hard disk to removable media.</td>
<td>The Full Disk Encryption preboot loads, but Windows does not.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This method is not recommended if Windows is functioning normally.</td>
<td></td>
</tr>
<tr>
<td>Repair CD</td>
<td>A bootable CD to decrypt a corrupted drive when the device cannot boot to the Full Disk Encryption preboot. A typical symptom of a corrupted disk is a black screen.</td>
<td>• The Full Disk Encryption preboot does not load.</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption cannot authenticate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do not use if Windows is functioning normally.</td>
<td></td>
</tr>
</tbody>
</table>
Repair CD

The Full Disk Encryption Repair CD is a bootable disk used to fully decrypt a device if the device is unable to boot.

**Note**

- If there is physical damage to the hard disk drive, the drive may not decrypt completely or may be unusable.
- If there are bad sectors in the hard disk drive, Endpoint Encryption will attempt to skip the bad sectors during decryption, which will lower performance depending upon the amount of bad sectors. If the bad sectors are in critical locations, the hard disk drive may be unusable.
- Make sure that the hard-disk drive cable is properly connected before booting from the Repair CD.

Repair CD Options

The following tables explain the options available in the Full Disk Encryption Repair CD. Use the tables to understand how to properly use the features available after booting into the Full Disk Encryption Repair CD.

**Basic Repair CD Options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Console</td>
<td>Launches Recovery Console.</td>
</tr>
<tr>
<td>Unlock Device</td>
<td>Unlock a device that has been locked because:</td>
</tr>
<tr>
<td></td>
<td>• too many unsuccessful login attempts</td>
</tr>
<tr>
<td></td>
<td>• no communication with PolicyServer for a specified duration</td>
</tr>
</tbody>
</table>

**Note**

Unlock option is only available when the policy Remote Authentication is set to **Lock Out**.
Reboot Computer

Restarts the device.

Advanced Options

Provides access to advanced options:
• Remove Full Disk Encryption Preboot
• Erase
• Force Decryption

Advanced Repair CD Options

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Preboot</td>
<td>Remove the Full Disk Encryption Preboot authentication screen from the device.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong> This action cannot be undone, and does not decrypt the drive. Use the Decrypt Disk to remove encryption.</td>
</tr>
<tr>
<td>Erase Disk</td>
<td>Remove all data from the drive.</td>
</tr>
<tr>
<td>Force Decryption</td>
<td>Decrypt the drive when Full Disk Encryption will not boot.</td>
</tr>
<tr>
<td>Return to the Main Menu</td>
<td>Return to the standard CD options.</td>
</tr>
</tbody>
</table>

**WARNING!**

Data loss may occur if Advanced Options are incorrectly used.

Recovering Data with the Repair CD

Use the Repair CD to attempt to recover data from an encrypted device. However, keep in mind a number of considerations before trying to decrypt the Endpoint Encryption device:
Only use the Repair CD if the Endpoint Encryption device is encrypted, or has begun encryption.


Do not attempt to decrypt a laptop unless it is connected to AC power.

If the Repair CD does not boot, verify that the Endpoint Encryption device has the latest BIOS version installed. Upgrade the system BIOS if necessary.

Drive decryption takes at least as long as the initial encryption process.

If the Repair CD encounters a bad sector, visible progress may slow down. Allow the Repair CD to continue decryption and contact Trend Micro Support before interrupting the process.

**WARNING!**

Do not interrupt the process after initiating decryption from the Repair CD. Irreversible data loss may occur.

**Decrypting a Disk with the Repair CD**

**Procedure**

1. Power on the endpoint.
   a. Immediately press F12 (or the appropriate button to enter the boot options).
   b. Insert the Repair CD and select the CD/DVD drive from the boot options screen.

   The device boots into the Repair CD environment.
The Full Disk Encryption Repair CD preboot logon appears.

**FIGURE 14-7. Full Disk Encryption Repair CD Preboot**

2. Specify the user name and password.
3. Click **Login**.
The Full Disk Encryption Repair CD menu screen appears.

![Full Disk Encryption Repair CD Menu Screen](image)

**Figure 14-8. Full Disk Encryption Repair CD**

4. Click **Recovery Console**.
The **Decrypt Disk** screen appears.

**Figure 14-9. Recover Console**

5. Click **Decrypt** to begin fully decrypting the Endpoint Encryption device.

6. When decryption completes, click **Exit** to return to the Repair CD menu.

7. Click **Reboot Computer** to restart the Endpoint Encryption device.

---

**Note**

Remove the Full Disk Encryption Repair CD from the optical drive to start the Endpoint Encryption device normally.

8. Log on to the Full Disk Encryption preboot.
9. Log on to Windows and proceed with the preferred recovery method.

Cleaning Up Full Disk Encryption Files

Decrypting a drive removes MBR changes and other essential elements used to protect the Endpoint Encryption device. For software encryption, decrypt the disk completely before uninstalling Full Disk Encryption. Otherwise, the operating system may have a critical error.

Procedure

• From a command line:
  a. Run `msiexec.exe /X{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}`.

• From Windows:
  a. Open `regedit.exe` within Windows and browse to the following key:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall \{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}
```

  b. Browse to the `UninstallString` key:

```
Example: msiexec.exe /x
{17BACE08-76BD-4FF5-9A06-5F2FA9EBDDEA}
```

c. Copy the string.

d. Open Run... and paste the string in the Open field.

e. Click OK.

   The Windows Installer window appears.

f. At the uninstall confirmation, click Yes.

---

**Note**

If the User Account Control window appears, click Allow.
g. When prompted to turn off DrAService, select the second radio button option **Do not close applications** and then click **OK**.

h. If prompted to reboot the endpoint, click **Yes**. Otherwise, manually restart the endpoint.

---

**Patch Management with Full Disk Encryption**

Use the Command Line Helper and DAAutoLogin together to run Windows patch management on devices with Full Disk Encryption installed. Command Line Helper creates encrypted values for scripts and DAAutoLogin grants a one-time bypass of the Full Disk Encryption Preboot.

Use DAAutoLogin in various combinations to accomplish different needs. Patches can be pushed out, and followed by a script using DAAutoLogin to send a reboot command for the device to display the Windows GINA for confirmation of successful patching or to another round of patches can be deployed.

DAAutoLogin accepts the following switches:

DAAutoLogin <pre-boot Username> <pre-boot Password> [ <Domain Name> <Domain Username> <Domain Password> ]

Each required value can be passed and separated with a space. Adding in the domain switches allows for Windows authentication.

---

**Note**

- Make sure to run both tools on a Full Disk Encryption device.
- Both tools are available in the tools folder of the zip file received from Trend Micro. For assistance, contact Trend Micro Support.

---

**Using Command Line Helper**

Administrators can use the Command Line Helper and DAAutoLogin together for seamless Full Disk Encryption patch management. Command Line Helper enables
encrypted values to pass via the installation script to the Full Disk Encryption preboot. 
DAAutoLogin grants a one-time bypass of the Full Disk Encryption preboot.

---

**Procedure**

1. Copy `CommandLineHelper.exe` locally to Full Disk Encryption device.
   
   Example: Copy `CommandLineHelper.exe` to the `C:` drive.

2. Open command prompt and type `C:\CommandLineHelper.exe`, then specify the user name or password.
   
   For example, use the following command if the user name is SMSUser:
   
   `C:\CommandLineHelper.exe SMSUser`

3. Press ENTER to display the encrypted value.

4. Run Command Line Helper again for the second encrypted value. If the first time was the user name, run it again to encrypt the password.

---

**Patching Process for Full Disk Encryption**

---

**Procedure**

1. Push patches to targeted Full Disk Encryption devices.

2. Follow up with a script using DAAutoLogin.

3. Send a reboot command for the Full Disk Encryption device to load Windows GINA for confirmation of successful patching or to push another round of patches.
Chapter 15

Encryption Management for Third-Party Products

A key feature of Full Disk Encryption is the ability to manage third-party encryption products. The Endpoint Encryption agents fully integrate with the encryption solutions built into the host operating systems.

Topics include:

• *About Encryption Management Agents on page 15-2*
• *Encryption Management Agent Policy Limitations on page 15-3*
• *Encryption Management for Microsoft BitLocker on page 15-4*
• *Encryption Management for Apple FileVault on page 15-10*
# About Encryption Management Agents

The following table explains the two Full Disk Encryption agents for third-party product encryption management.

---

Note

For information about all available Endpoint Encryption agents, see *Endpoint Encryption Agents on page 1-14.*

---

**TABLE 15-1. Encryption Management Agents**

<table>
<thead>
<tr>
<th>AGENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Encryption Management for Microsoft BitLocker | The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint.  

Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure.  

For more information, see *About Full Disk Encryption on page 14-2.* |
| Encryption Management for Apple FileVault | The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint.  

Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure.  

For more information, see *About Full Disk Encryption on page 14-2.* |
Encryption Management Agent Policy Limitations

The following table explains the policy limitations for Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker. To use all policies, install the Full Disk Encryption agent instead.

**Note**

Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

The following table explains the policies affecting each agent. Use it to understand the policy limitations of third-party agents.

**Table 15-2. Policies Affecting Full Disk Encryption Agents**

<table>
<thead>
<tr>
<th>POLICY</th>
<th>FULL DISK ENCRYPTION</th>
<th>ENCRYPTION MANAGEMENT FOR APPLE FILEVAULT</th>
<th>ENCRYPTION MANAGEMENT FOR MICROSOFT BITLOCKER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow User Recovery</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow User to Uninstall</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypt Device</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Account Lockout Action</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Lockout Period</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dead Man Switch</td>
<td>●</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Encryption Management for Microsoft BitLocker

Encryption Management for Microsoft BitLocker manages BitLocker Drive Encryption™ (BDE) for endpoints running Microsoft Windows 7 Ultimate and Enterprise editions and Windows 8 Pro and Enterprise editions. Encryption Management for Microsoft BitLocker is designed to protect data by providing

<table>
<thead>
<tr>
<th>Policy</th>
<th>Full Disk Encryption</th>
<th>Encryption Management for Apple FileVault</th>
<th>Encryption Management for Microsoft BitLocker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Locked Action</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Killed Action</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Failed Login Attempted Allowed</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If Found</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Notice</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Lock Device Time Delay</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preboot Bypass</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Info</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Token Authentication</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Methods Allowed</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync Interval</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
encryption for entire volumes. By default, BDE uses the AES encryption algorithm in CBC mode with a 128-bit or 256-bit key.

**Viewing Encryption Status**

**Procedure**

1. Click the Full Disk Encryption icon ( ).
   - For Windows, go to the system tray.
   - For Mac OS, go to the menu bar.

2. Open the **Encryption Status** tab.

3. See *Understanding Encryption Status on page 15-6* for details.
Understanding Encryption Status

The **Encryption Status** tab provides details about the encrypted drives, the types of encryption, and the ratio that the drive is encrypted or not encrypted. See the figure and description below for more information.

![Encryption Management for Microsoft BitLocker](image_url)

**TABLE 15-3. Device Encryption Status**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pie Chart</td>
<td>The pie chart represents the ratio that the hard disk is encrypted and not encrypted.</td>
</tr>
<tr>
<td>Drive</td>
<td>The hard disk with the agent installed.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The percentage that the drive is encrypted.</td>
</tr>
<tr>
<td>Action</td>
<td>The current encryption status.</td>
</tr>
</tbody>
</table>
## Encryption Management for Third-Party Products:

### Understanding Agent Information

The **Information** tab provides detailed information about the user account, Endpoint Encryption device, and policy synchronization. See the figure and description below for more information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>The type of encryption deployed on the endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker always use software-based encryption.</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>Whether FIPS is enabled. For information about FIPS, see <em>About FIPS</em> on page 1-7.</td>
</tr>
</tbody>
</table>
### TABLE 15-4. Agent Information

<table>
<thead>
<tr>
<th>LABEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMEE user name</td>
<td>The Endpoint Encryption account used to log on the Endpoint Encryption device. This is different from the Windows logon.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The unique ID that identifies the agent and endpoint to PolicyServer.</td>
</tr>
<tr>
<td>Operating system</td>
<td>The operating system and version currently installed on the endpoint.</td>
</tr>
<tr>
<td>Computer name</td>
<td>The endpoint computer name to identify it on the network.</td>
</tr>
<tr>
<td>Last sync</td>
<td>The timestamp for the last policy synchronization to PolicyServer. For details about synchronizing policies, see Synchronizing Policies From the Menu Bar on page 15-15.</td>
</tr>
<tr>
<td>Sync with PolicyServer</td>
<td>Forces an immediate policy update.</td>
</tr>
</tbody>
</table>

#### Synchronizing Policies with PolicyServer

There are two ways to synchronize policies with PolicyServer. For information about policies affecting Encryption Management for Microsoft BitLocker devices, see Encryption Management Agent Policy Limitations on page 15-3.

- Synchronizing Policies From the Menu Bar on page 15-15
- Synchronizing Policies from the About Screen on page 15-9

#### Automatic Policy Synchronization

The following list explains the events that initiate policy synchronization between all Endpoint Encryption agents and PolicyServer.

- After the operating system loads and the Endpoint Encryption agent service starts
Note
For information about Endpoint Encryption services, see Endpoint Encryption Services on page C-1.

- When the Full Disk Encryption preboot starts (Full Disk Encryption only)
- The time duration of the Sync Interval policy elapses

Open the About screen in the Endpoint Encryption agent to manually synchronize policies.

Note
Endpoint Encryption device actions initiate after the Endpoint Encryption agent receives policy updates.

Synchronizing Policies from the About Screen

For information about policies limitations affecting the Encryption Management for Microsoft BitLocker agent, see Encryption Management Agent Policy Limitations on page 15-3.

Procedure

1. Make sure that the Endpoint Encryption device has network access.
2. Click the agent icon.
3. Select About Full Disk Encryption to open the agent menu.
4. Open the Information tab.
5. Click Sync with PolicyServer.

If successful, all Endpoint Encryption policies are up-to-date.
Synchronizing Policies From the System Tray

Procedure

1. Make sure that the Endpoint Encryption device has network access.
2. Click the agent icon (lenmiş).

If successful, all Endpoint Encryption policies are up-to-date.

Encryption Management for Apple FileVault

Encryption Management for Apple FileVault manages Apple Filevault™ to encrypt the entire OS X startup volume, which typically includes the home directory, abandoning the disk image approach. Encryption Management for Apple FileVault manages encryption using Apple FileVault with the user's password as the encryption pass phrase. Encryption Management for Apple FileVault uses the AES-XTS mode of AES with 128 bit blocks and a 256 bit key to encrypt the disk, as recommended by NIST. Only unlock-enabled users can start or unlock the drive. Once unlocked, other users may also use the computer until it is shut down.

Viewing Encryption Status

Procedure

1. Click the Full Disk Encryption icon (ambahş).
   - For Windows, go to the system tray.
   - For Mac OS, go to the menu bar.
2. Open the Encryption Status tab.
3. See Understanding Encryption Status on page 15-6 for details.

Understanding Encryption Status

The Encryption Status tab provides details about the encrypted drives, the types of encryption, and the ratio that the drive is encrypted or not encrypted. See the figure and description below for more information.

![Encryption Status Tab](image)

**TABLE 15-5. Device Encryption Status**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pie Chart</td>
<td>The pie chart represents the ratio that the hard disk is encrypted and not encrypted.</td>
</tr>
<tr>
<td>Drive</td>
<td>The hard disk with the agent installed.</td>
</tr>
<tr>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The percentage that the drive is encrypted.</td>
</tr>
<tr>
<td>Action</td>
<td>The current encryption status.</td>
</tr>
<tr>
<td>Average speed</td>
<td>The rate (MB/second) that the drive is encrypting or decrypting.</td>
</tr>
<tr>
<td>Estimated time</td>
<td>The amount of time until the drive is 100% encrypted or decrypted.</td>
</tr>
</tbody>
</table>

Understanding Agent Information

The **Information** tab provides detailed information about the user account, Endpoint Encryption device, and policy synchronization. See the figure and description below for more information.
### Table 15-6. Agent Information

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMEE user name</td>
<td>The Endpoint Encryption account used to log on the Endpoint Encryption device. This is different from the Windows logon.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The unique ID that identifies the agent and endpoint to PolicyServer.</td>
</tr>
<tr>
<td>Operating system</td>
<td>The operating system and version currently installed on the endpoint.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>The endpoint computer name to identify it on the network.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>The Enterprise name of the PolicyServer managing agent policies.</td>
</tr>
<tr>
<td>Last sync</td>
<td>The timestamp for the last policy synchronization to PolicyServer. For details about synchronizing policies, see <em>Synchronizing Policies From the Menu Bar on page 15-15</em>.</td>
</tr>
<tr>
<td>Synchronize now</td>
<td>Forces an immediate policy update.</td>
</tr>
</tbody>
</table>

### Synchronizing Policies with PolicyServer

There are two ways to synchronize policies with PolicyServer. For information about policies affecting Encryption Management for Apple FileVault devices, see *Encryption Management Agent Policy Limitations on page 15-3*.

- *Synchronizing Policies from the About Screen on page 15-14*
- *Synchronizing Policies From the Menu Bar on page 15-15*

### Automatic Policy Synchronization

The following list explains the events that initiate policy synchronization between all Endpoint Encryption agents and PolicyServer.

- After the operating system loads and the Endpoint Encryption agent service starts
Note
For information about Endpoint Encryption services, see *Endpoint Encryption Services on page C-1*.

- When the Full Disk Encryption preboot starts (Full Disk Encryption only)
- The time duration of the **Sync Interval** policy elapses

Open the **About** screen in the Endpoint Encryption agent to manually synchronize policies.

Note
Endpoint Encryption device actions initiate after the Endpoint Encryption agent receives policy updates.

### Synchronizing Policies from the About Screen

For information about policies limitations affecting Encryption Management for Apple FileVault agents, see *Encryption Management Agent Policy Limitations on page 15-3*.

**Procedure**

1. Make sure that the Endpoint Encryption device has network access.
2. Click the agent icon (_bold).
3. Select **About Full Disk Encryption** to open the agent menu.
4. Open the **Information** tab.
5. Click **Synchronize now**.

If successful, all Endpoint Encryption policies are up-to-date.
Synchronizing Policies From the Menu Bar

Procedure

1. Make sure that the Endpoint Encryption device has network access.
2. Click the agent icon.
3. Select **Synchronize Policies**.

If successful, all Endpoint Encryption policies are up-to-date.
Part V

Advanced Management and Technical Support
Chapter 16

Advanced Enterprise Features

In environments primarily managed by Control Manager, use PolicyServer MMC for advanced options including certain reports, logs, and maintenance. Endpoint Encryption keeps comprehensive logs and generates reports about events and updates. Use logs and reports to assess policy controls and to verify component updates. Enterprise maintenance provides a way to purge inactive users, inactive devices, and logs matching specific criteria from the database.

Topics include:

- Enterprise Maintenance on page 16-2
- Restoring Deleted Users and Devices on page 16-10
- Enterprise Log Events on page 16-11
- Enterprise Reports on page 16-15
Enterprise Maintenance

PolicyServer records system activities (changes made to policies, successful authentication attempts, devices locked due to too many unsuccessful logon attempts) and maintains those records as log events. You can generate reports on an as-needed or scheduled basis.

PolicyServer MMC has a variety of built-in reports to verify device encryption status, user/device activity, and PolicyServer integrity.

---

**Note**

Only Enterprise Administrator accounts can use reports.

---

Purge Inactive Users

An inactive user is a user account that has not logged on any Endpoint Encryption devices for a specified time period.

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.

---

**WARNING!**

Purged user accounts cannot authenticate to any Endpoint Encryption devices.

---

Purging Inactive Users

**Procedure**

1. Log on to PolicyServer MMC.

2. Expand the Enterprise, then go to Enterprise Maintenance.

3. Click Purge Inactive Users.
4. Specify the number of days to purge all user accounts that have not logged on a device for period of time.

   **Note**
   Specify a range between 7 and 999 days.

5. Click **Purge**.

6. Click **OK** to confirm the purge.

Anything meeting the purge criteria is deleted from the database.

**Viewing the Purge Inactive Users Log Event**

**Procedure**

1. Log on to PolicyServer MMC.

2. Click **Enterprise Log Events**.

   All current log events appear in the right pane.

3. At the bottom of the page, click **Filter**.
The Search Filter window appears.

![Search Filter Window]

4. From the Message ID drop-down list, select 200105, Inactive Users Removed from Enterprise.

5. Click Search.

   All log event matching the specified criteria appear.

6. Double-click a log event.

   The Log Record window appears displaying all log data for the selected event.

---

**Viewing the Purge Inactive Users Report**

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.

3. Click **Enterprise Scheduled Reports**.

4. Do one of the following in the right pane:
   - To view the report in tabular format, double-click **Purged Inactive Users**.
   - To view the report in HTML format, right-click a report and then select **Display Report**.

### Purge Inactive Devices

An inactive device is any Endpoint Encryption device that has not been logged on for a specified time period.

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.

---

**WARNING!**

Users cannot log on to purged Endpoint Encryption devices.

---

### Purging Inactive Devices

**Procedure**

1. Log on to PolicyServer MMC.

2. Expand the Enterprise, then go to **Enterprise Maintenance**.

3. Click **Purge Inactive Devices**.

4. Specify the number of days to purge all user accounts that have not logged on any Endpoint Encryption device for period of time.

5. Click **Purge**.
6. Click **OK** to confirm the purge.

Anything meeting the purge criteria is deleted from the database.

**Viewing the Purge Inactive Devices Log Event**

**Procedure**

1. Log on to PolicyServer MMC.
2. Click **Enterprise Log Events**.
   
   All current log events appear in the right pane.
3. At the bottom of the page, click **Filter**.
   
   The **Search Filter** window appears.
4. From the **Message ID** drop-down list, select **200303, Inactive Devices Removed from Enterprise**.

5. Click **Search**.

   All log event matching the specified criteria appear.

6. Double-click a log event.

   The **Log Record** window appears displaying all log data for the selected event.

---

**Viewing the Purged Inactive Devices Report**

**Procedure**

1. Log on to PolicyServer MMC.

2. Expand the Enterprise, then go to **Enterprise Maintenance**.

3. Click **Enterprise Scheduled Reports**.

4. Do one of the following in the right pane:

   - To view the report in tabular format, double-click **Purged Inactive Devices**.
   - To view the report in HTML format, right-click a report and then select **Display Report**.

   The report appears.

---

**Log Purge**

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.
Purging the Log Database

Procedure

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to Enterprise Maintenance.
3. Click Purge Log Database.
4. Select Enable scheduled purge.
5. Configure the following options:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge logs older than &lt;X&gt; days</td>
<td>Specify the number of days to keep logs. Anything older than the specified</td>
</tr>
<tr>
<td></td>
<td>number of days is purged.</td>
</tr>
<tr>
<td>Interval type</td>
<td>Select to purge the log database daily, weekly, biweekly, or monthly.</td>
</tr>
<tr>
<td>Start date</td>
<td>Select when to start the scheduled purge.</td>
</tr>
<tr>
<td>Time</td>
<td>Specify the time of day for the scheduled purge.</td>
</tr>
</tbody>
</table>

6. Click Apply.
7. At the confirmation message, click OK.

Anything meeting the purge criteria is deleted from the database.

Viewing the Log Database Purge Event

Note

The log database purge only occurs once the schedule criteria has been met. If no data matches the search criteria, verify that the schedule is correctly set. For details, see Purging the Log Database on page 16-8.
Procedure

1. Log on to PolicyServer MMC.
2. Click **Enterprise Log Events**.

   All current log events appear in the right pane.

3. At the bottom of the page, click **Filter**.

   The **Search Filter** window appears.

4. From the **Message ID** drop-down list, select **103104, Log data purged from Enterprise**.

5. Click **Search**.

   All log event matching the specified criteria appear.

6. Double-click a log event.
The Log Record window appears displaying all log data for the selected event.

Restoring Deleted Users and Devices

Use the PolicyServer MMC Recycle Bin to restore a deleted Endpoint Encryption user or device. All deleted Endpoint Encryption users and devices are stored in the Recycle Bin at the Enterprise level. Groups do not have a recycle bin. Restoring a deleted Endpoint Encryption user or device does not add it back to previously assigned policy groups.

Restoring a Deleted User

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption user.

Procedure

1. Log on to PolicyServer MMC.
2. Expand the Recycle Bin.
3. Open Deleted Users.
   The right pane loads all deleted users.
4. Right-click the user account, then select Restore User.
   The user is added back to the Enterprise, but does not belong to any policy groups.

Restoring a Deleted Device

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption device.
**Enterprise Log Events**

PolicyServer records log events using predefined criteria including access attempts, system errors, modifications to users or groups, policy changes, and compliance issues. Managing log events and reports allows Enterprise Administrator and Group Administrator accounts to search for specific log events and report about server and client security.

**Managing Log Events**

Only messages within the last seven (7) days automatically display. Use the filter to view older log events. It is useful to search the logs using the message ID. For example, searching for the message ID “400008” displays all “Device Encryption Complete” messages. For information about message IDs, see *PolicyServer Message IDs on page B-1*.

**Procedure**

1. Log on to PolicyServer MMC.
2. Select a log event level:
For enterprise-level logs, expand **Enterprise Log Events**.

For group-level logs, go to **Group Name > Log Events**.

The log window appears. All log events for the past seven (7) days automatically display.

3. Double-click any log to view details.

4. Click **Filter** to search the log file:
   a. Specify the search criteria.
   b. Select the date range.
   c. Click **Search**.

5. Click **Refresh** to update log data.

6. Click **Previous** or **Next** to navigate through log data.

---

### Alerts

You can customize alert criteria using predefined security levels to help categorize alerts. Send log events to individual or multiple email recipients by setting alerts at the enterprise or group.

---

**Note**

For information about message IDs, see *PolicyServer Message IDs on page B-1*.

---

### Setting PolicyServer Alerts

**Procedure**

1. Log on to PolicyServer MMC.
2. Select a log event level:
• For enterprise-level logs, expand Enterprise Log Events.
• For group-level logs, go to Group Name > Log Events.

The log window appears. All log events for the past seven (7) days automatically display.

3. Click Alerts.
4. In the right pane whitespace, right-click and select Add.

The Edit Alert window appears.
5. Specify an Alert Name.
6. Select the severity of logs that trigger alerts.
7. Select the message IDs to trigger alerts.
8. Specify one email address per line to send the alert notification.
9. Select whether to send alerts based on the number of events in a set time.
10. Click Done.

Enabling PolicyServer to relay SMS and Email Delivery

This function only works for PolicyServer installed on Windows Server 2008 or Windows Server 2008 R2.

Procedure
1. Log on to the Windows server.
2. Open Server Manager.
3. Go to Features > Add Features.

The Add role services and features required for SMTP Server window appears.
5. Click Add Required Role Services.
6. Click Next.
7. Click Next again.
8. Click Install.
   The Web Server IIS and SMTP Server installs.
9. Click Close.
10. Go to Start > Administrative Tools > Internet Information Services (IIS) 6.0 Manager.
    IIS 6.0 Manager opens.
11. Expand ServerName (local device).
12. Right-click [SMTP Virtual Server #1] and click Properties.

   **Note**
   Mark Enable logging for future troubleshooting.

13. Go to Access > Connection... and select Only the list below, and then click Add....
14. In the IP address field, specify 127.0.0.1, then click OK.

   **Note**
   Repeat to specify all IP addresses on local server

15. Click OK.
16. Go to Delivery > Advanced... and specify the Masquerade domain in the following format: psproxy.<domain>.<com/org>.
17. Click OK twice to close the SMTP Virtual Server #1 Properties window.
18. Go to Enterprise Policies > PolicyServer > PDA > Email.
19. Open SMTP ServerName, specify 127.0.0.1, then click Apply.
Configuring Advanced Premise

For best results, create a Sender Policy Framework (SPF) DNS entry. To create an SPF record in other DNS Servers (BIND), consult the vendor documentation.

Procedure

1. On a Windows DNS Server, open DNS Management Console.
2. Right-click the forward lookup zone for the domain, and select Other New Records.
3. Scroll down and select TEXT (TXT).
4. Leave Record Name blank, and specify:
   \[v=spf1 ip4:<external_PolicyServer_IP_address> -all\]
5. Click OK.

Enterprise Reports

PolicyServer records log events using predefined criteria including access attempts, system errors, modifications to users or groups, policy changes, and compliance issues. Managing log events and reports allows Enterprise Administrator and Group Administrator accounts to search for specific log events and report about server and client security. Enterprise Administrator accounts can generate reports on an as-needed or scheduled basis.

PolicyServer MMC has a variety of built-in reports to verify Endpoint Encryption device encryption status, Endpoint Encryption user or device activity, and PolicyServer integrity.

Note

Only the Enterprise Administrator can use reports.
Report Options

The following table describes the options available for different reports. Right-click a report to view available options.

<table>
<thead>
<tr>
<th>REPORT OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>Remove all information displayed in the results window; it does not delete the information.</td>
</tr>
<tr>
<td>Display Error</td>
<td>View a description of the error causing the report to be invalid.</td>
</tr>
<tr>
<td>Display Report</td>
<td>View the report.</td>
</tr>
<tr>
<td>Next Page</td>
<td>Move to the next page of the search items.</td>
</tr>
<tr>
<td>Previous Page</td>
<td>Return to the previous page of the search items.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the status of a submitted report.</td>
</tr>
<tr>
<td>Remove Report</td>
<td>Delete the report.</td>
</tr>
<tr>
<td>Schedule Report</td>
<td>Set up a schedule for the report to be run on a specific day or time.</td>
</tr>
<tr>
<td>Submit Report</td>
<td>Generate the selected report.</td>
</tr>
</tbody>
</table>

Report Icons

The following table describes the icons that may appear next to a report.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Standard Icon" /></td>
<td>Standard reports can be submitted on an as-needed basis to view statistics and other usage metrics.</td>
</tr>
<tr>
<td><img src="image" alt="Alert Icon" /></td>
<td>Alert reports notify Enterprise Administrator accounts about potential security issues.</td>
</tr>
</tbody>
</table>
Report Types

Reports make log information easier to understand. PolicyServer MMC separates reports into two distinct categories:

- **Standard reports**: Standard reports capture specific log information in a report format. Submit standard reports on an as-needed basis.

- **Alert reports**: Alert reports send an alert notification to the Enterprise Administrator and capture the security incident in a report.

---

**Note**

Only the Enterprise Administrator can use reports.

---

Standard Reports

Use the following table to understand which standard reports are available to generate as needed.

**Table 16-1. List of Standard Reports**

<table>
<thead>
<tr>
<th>REPORT NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Encryption Status</td>
<td>Reports the encryption status for all Endpoint Encryption devices in the Enterprise.</td>
</tr>
<tr>
<td>Device Operating System Count</td>
<td>Reports all device operating systems and the count for each.</td>
</tr>
<tr>
<td>Device Version Count</td>
<td>Reports all Endpoint Encryption device versions and the count for each.</td>
</tr>
<tr>
<td>Devices By Last Sync Date</td>
<td>Reports all Endpoint Encryption devices that synchronized with PolicyServer in the last x amount of days.</td>
</tr>
<tr>
<td>Devices Not Communicating</td>
<td>Reports the Endpoint Encryption devices that have not communicated in the last &lt;X&gt; days.</td>
</tr>
<tr>
<td>Devices with Last Logged in User</td>
<td>Reports all Endpoint Encryption devices and the last user to have authenticated to it.</td>
</tr>
</tbody>
</table>
### Running Standard Reports

Standard reports capture specific log information in a report format. Submit standard reports on an as-needed basis.

**Procedure**

1. Right-click the desired report, then select **Submit Report**.
2. Specify report parameters if required, then click **Apply**.
   
   The report appears.
3. To view the report, go to **Enterprise Reports > Enterprise Submitted Reports**.

<table>
<thead>
<tr>
<th>REPORT NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Available License</td>
<td>Reports the days left in the license, available Endpoint Encryption devices and users, and count of used devices and users.</td>
</tr>
<tr>
<td>Enterprise Inactive User</td>
<td>Reports all Endpoint Encryption users who have not logged on to Endpoint Encryption devices for a specified time period.</td>
</tr>
<tr>
<td>Enterprise User Activity</td>
<td>Reports total Endpoint Encryption devices, total Endpoint Encryption users, and PolicyServer MMC user count along with Endpoint Encryption device activity.</td>
</tr>
<tr>
<td>Full Disk Encryption Device Not 100% Encrypted</td>
<td>Reports all Endpoint Encryption devices in the last &lt;X&gt; days that started encrypting but did not finish.</td>
</tr>
<tr>
<td>User Activity By Day</td>
<td>Reports the Endpoint Encryption user activity within &lt;X&gt; amount of days for the given user.</td>
</tr>
<tr>
<td>Users Added</td>
<td>Reports all Endpoint Encryption users added within the last &lt;X&gt; days.</td>
</tr>
<tr>
<td>Users Never Logged into a Device</td>
<td>Reports all Endpoint Encryption users who have never authenticated to any Endpoint Encryption device.</td>
</tr>
</tbody>
</table>
Alert Reports

Use the following table to understand when PolicyServer generates an alert report.

<table>
<thead>
<tr>
<th>ALERT NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consecutive Failed Logon Attempts on a Single Device</td>
<td>An alert is sent when multiple, consecutive authentication attempts to any Endpoint Encryption device have all failed.</td>
</tr>
<tr>
<td>Log Integrity Alert</td>
<td>An alert is sent when there is an indication that the PolicyServer logs have been tampered with.</td>
</tr>
<tr>
<td>Policy Tampering Alert</td>
<td>An alert is sent when PolicyServer detects that an entity has tampered with policies.</td>
</tr>
<tr>
<td>Primary and Secondary Action Enforced</td>
<td>An alert is sent when PolicyServer has had no connection, and the primary or secondary action has been enforced.</td>
</tr>
</tbody>
</table>

Running Alert Reports

To view the generated report, go to Enterprise Reports > Enterprise Submitted Reports.

Procedure

1. Right-click the desired alert report, then select Configure Alerts.

   The Alerts Configuration window appears.

2. Specify the SMTP Server Address and the Sender that will process the outgoing email message.

3. Click Apply.

4. Right-click the desired report and select Submit Alert.
Displaying Reports

**Note**
Only the Enterprise Administrator can use reports.

**Procedure**
1. Go to Enterprise Reports > Enterprise Submitted Reports.
2. Right-click desired report, then select Display Report.
   The report appears.
3. To export the report, click the Save icon and then select Excel or Acrobat (PDF) file.

Scheduling Reports

Schedule a report to automatically run at any specific date and time.

**Procedure**
1. Open Enterprise Reports.
2. Right-click the desired report, then select Schedule Report.
   The Report Parameters window displays.
3. Specify the report parameters, then click Apply.
   The Report Scheduler displays.
4. Specify the report interval, date and time, then click Apply.
   The report is scheduled.
5. To view scheduled reports, go to Enterprise Reports > Enterprise Scheduled Reports.

Displaying Report Errors

Sometimes an error prevents a report from correctly running. To view PolicyServer message IDs, see PolicyServer Message IDs on page B-1.

Procedure

1. Go to Enterprise Reports > Enterprise Submitted Reports.
2. Right-click the report with an error, then select Display Error.

The report error message displays.
Chapter 17

Maintenance and Technical Support

The following topics describe how to understand the Maintenance Agreement, find solutions online, use the Support Portal, contact Trend Micro, and find additional resources.

Topics include:

• Maintenance Agreement on page 17-2
• Troubleshooting Resources on page 17-5
• Contacting Trend Micro on page 17-7
• Other Resources on page 17-8
**Maintenance Agreement**

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

[Online Registration System](#)

**Renewing the Maintenance Agreement**

Trend Micro or an authorized reseller provides technical support, downloads, and program updates for one (1) year to all registered users, after which renewal maintenance must be purchased.

If the Maintenance Agreement expires, basic operations are maintained; however, new users and devices cannot be added to PolicyServer, either through the PolicyServer MMC, agent installations, or Control Manager. To prevent this, renew the Maintenance Agreement as soon as possible.

For customers upgrading, the existing license is accepted until the expiration.
Procedure

1. To renew the Maintenance Agreement, do one of the following:
   • To purchase renewal maintenance, contact the same vendor from whom the product was purchased. A Maintenance Agreement extending protection for another year will be sent by post to the primary company contact listed in your Registration Profile.
   • To view or modify the company’s Registration Profile, log on at the Trend Micro online registration website: https://olr.trendmicro.com/registration/us/en-us

2. To view the Registration Profile, specify the Logon ID and password created when the product was first registered with Trend Micro (as a new customer), and then click Login.

3. To update the environment with the new Activation Code, see Activating the New Product License on page 17-3.

Trial License

You can install and evaluate Endpoint Encryption for a limited 30-day trial period. During PolicyServer installation, the Enterprise database and Enterprise Administrator account are created. PolicyServer functions normally with all client applications, unlimited devices, and up to 100 users for the 30-day trial period. After 30 days, contact Trend Micro Technical Sales to receive a license file. Endpoint Encryption user accounts and devices function normally after the trial period expires.

Activating the New Product License

A free 30-day trial license is available to install and evaluate Endpoint Encryption. If activating from the trial license, make sure to upgrade to the full version before the license expires.

Procedure

1. Log on to the server where PolicyServer is currently installed.
2. Go to the folder containing the PolicyServer program files and open the Tools folder.

3. Run TMEE_License_Renewal.exe.

The License Renewal Tool opens.

4. Under Renew License, click Renew Online to access the Trend Micro registration website.

After completing the registration, Trend Micro sends an email message containing the Activation Code.

5. Specify the new Activation Code for the product.

6. Click Activate.

7. At the confirmation message, click OK to continue.

8. Click Exit.

The updated Endpoint Encryption product license is immediately available.

**Viewing the Product License**

Use PolicyServer MMC to view the current license status.

**Procedure**

1. Log on to PolicyServer MMC.

2. Right-click the Enterprise and select Activation/License.

The Registration Information screen appears.

3. Review the following options.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>For a full licence, the Activation Code appears. For other license types, the name of the license appears.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>The date that the license was activated.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date that the license must be renewed. After a license expires, existing Endpoint Encryption users can still log on to Endpoint Encryption devices, but no new Endpoint Encryption devices or users can be added to the Enterprise.</td>
</tr>
<tr>
<td>Number of Devices</td>
<td>The number of Endpoint Encryption devices allowed in the license.</td>
</tr>
<tr>
<td>Number of Installed Devices</td>
<td>The number of Endpoint Encryption devices currently configured in the Enterprise.</td>
</tr>
<tr>
<td>Number of Users</td>
<td>The total number of Endpoint Encryption users allowed in the license.</td>
</tr>
<tr>
<td>Number of Created Users</td>
<td>The number of Endpoint Encryption users currently added to the Enterprise.</td>
</tr>
<tr>
<td>Activation Period in Days</td>
<td>The number of days left until the license expires.</td>
</tr>
</tbody>
</table>

4. Click Close.

### Product Maintenance

From time to time, Trend Micro might release a patch for a reported known issue or an upgrade that applies to the product. To find out whether there are any patches available, visit: [http://downloadcenter.trendmicro.com](http://downloadcenter.trendmicro.com)

Patches are dated. If there are available patches, open the readme file to determine whether the patch is applicable. If so, follow the upgrade instructions in the readme.

### Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.
Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

2. Select a product or service from the appropriate drop-down list and specify any other related information.
   The Technical Support product page appears.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Submit a Support Case from the left navigation and add any relevant details, or submit a support case here:
   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cybersecurity experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
• Threat reports, research papers, and spotlight articles
• Solutions, podcasts, and newsletters from global security insiders
• Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

• Malware and malicious mobile code currently active or "in the wild"
• Correlated threat information pages to form a complete web attack story
• Internet threat advisories about targeted attacks and security threats
• Web attack and online trend information
• Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)</td>
</tr>
<tr>
<td>Fax</td>
<td>+1 (408) 257-2003</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
</tbody>
</table>
Email address | support@trendmicro.com

- Worldwide support offices:
- Trend Micro product documentation:
  [http://docs.trendmicro.com](http://docs.trendmicro.com)

**Speeding Up the Support Call**

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

**Other Resources**

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.
TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:
Appendix A

Introducing Trend Micro™ Control Manager™

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up to date. Example update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter contains the following topics:

- Control Manager Standard and Advanced on page A-3
- Introducing Control Manager Features on page A-3
- Control Manager Architecture on page 3-3
- Registering Endpoint Encryption to Control Manager on page A-8
• Understanding User Access on page A-9
• Understanding the Product Directory on page A-15
• Downloading and Deploying New Components on page A-38
• Using Logs on page A-65
• Understanding Reports on page A-68
Control Manager Standard and Advanced

Control Manager is available in two versions: Standard and Advanced. Control Manager Advanced includes features that Control Manager Standard does not. For example, Control Manager Advanced supports a cascading management structure. This means the Control Manager network can be managed by a parent Control Manager Advanced server with several child Control Manager Advanced servers reporting to the parent Control Manager Advanced server. The parent server acts as a hub for the entire network.

Note
Control Manager Advanced supports the following as child Control Manager servers:
- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support see the Trend Micro Control Manager documentation.

Introducing Control Manager Features

Trend Micro designed Control Manager to manage antivirus and content security products and services deployed across an organization’s local and wide area networks.

Table A-1. Control Manager Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy management</td>
<td>System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Centralized configuration</td>
<td>Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console. These features help ensure consistent enforcement of your organization’s virus/malware and content security policies.</td>
</tr>
<tr>
<td>Proactive outbreak prevention</td>
<td>With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/malware outbreak.</td>
</tr>
<tr>
<td>Secure communication infrastructure</td>
<td>Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.</td>
</tr>
<tr>
<td>Secure configuration and component download</td>
<td>These features allow you to configure secure web console access and component download.</td>
</tr>
<tr>
<td>Task delegation</td>
<td>System administrators can give personalized accounts with customized privileges to Control Manager web console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.</td>
</tr>
<tr>
<td>Command Tracking</td>
<td>This feature allows you to monitor all commands executed using the Control Manager web console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.</td>
</tr>
<tr>
<td>On-demand product control</td>
<td>Control managed products in real time. Control Manager immediately sends configuration modifications made on the web console to the managed products. System administrators can run manual scans from the web console. This command system is indispensable during a virus/malware outbreak.</td>
</tr>
</tbody>
</table>
Centralized update control
Update virus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.

Centralized reporting
Get an overview of the antivirus and content security product performance using comprehensive logs and reports.
Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy. The following table provides a list of components Control Manager uses.
### Table A-2. Control Manager Components

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager server</td>
<td>Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features:</td>
</tr>
<tr>
<td></td>
<td>• An SQL database that stores managed product configurations and logs</td>
</tr>
<tr>
<td></td>
<td>Control Manager uses the Microsoft SQL Server database (db_ControlManager.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.</td>
</tr>
<tr>
<td></td>
<td>• A web server that hosts the Control Manager web console</td>
</tr>
<tr>
<td></td>
<td>• A mail server that delivers event notifications through email messages</td>
</tr>
<tr>
<td></td>
<td>Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure Event Center to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification.</td>
</tr>
<tr>
<td></td>
<td>• A report server, present only in the Advanced Edition, that generates antivirus and content security product reports</td>
</tr>
<tr>
<td></td>
<td>A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network.</td>
</tr>
</tbody>
</table>
**COMPONENT** | **DESCRIPTION**
--- | ---
Trend Micro Management Communication Protocol | MCP handles the Control Manager server interaction with managed products that support the next generation agent. MCP is the new backbone for the Control Manager system. MCP agents install with managed products and use one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.

Trend Micro Management Infrastructure | Handles the Control Manager server interaction with older managed products.

The Communicator, or the Message Routing Framework, is the communication backbone of the older Control Manager system. It is a component of the Trend Micro Management Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. They interact with Control Manager 2.x agents to communicate with older managed products.

Control Manager 2.x Agents | Receives commands from the Control Manager server and sends status information and logs to the Control Manager server.

The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Therefore, install agents on the same computer as managed products.

Web-based management console | Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™

The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget Framework</td>
<td>Allows an administrator to create a customized dashboard to monitor the Control Manager network.</td>
</tr>
</tbody>
</table>

Registering Endpoint Encryption to Control Manager

Before registering the Endpoint Encryption server to a Control Manager server, you must ensure that both the server and the Control Manager server belong to the same network segment.

Procedure

1. Click **Administration > Control Manager Settings**.

   **Note**
   
   Control Manager uses the name specified in the Host name field to identify the Endpoint Encryption server. The Host name appears in the Product Directory of Control Manager.

   The **Control Manager Settings** screen displays.

2. Under **Connection settings**, type the name of the Endpoint Encryption server in the **Entity display name** field.

3. Under **Control Manager Server Settings** specify the following:
   
   a. Type the Control Manager server IP address or host name in the Server FQDN or IP address field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.
d. If your network requires authentication, type the user name and password for your IIS server in the **Username** and **Password** fields.

e. If you use a NAT device, select **Enable two-way communication port forwarding** and type the NAT device’s IP address and port number in **IP address** and **port number**.

Refer to the *Trend Micro Control Manager Administrator’s Guide* for more information about managing products in Control Manager.

4. From the Control Manager management console, click **Products**.

The **Product Directory** screen appears.

5. The Endpoint Encryption server appears in the Product Directory tree.

---

**Understanding User Access**

Control Manager access control consists of the following four sections.

**TABLE A-3. Control Manager User Access Options**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Account</td>
<td>The <strong>My Account</strong> screen contains all the account information that Control Manager has for a specific user. The information on the <strong>My Account</strong> screen varies from user to user.</td>
</tr>
</tbody>
</table>
### User Accounts
The **User Accounts** screen displays all Control Manager users. The screen also provides the options for users to create and maintain Control Manager user accounts.

Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are:

- Execute
- Configure
- Edit Directory

### User Roles
The **User Roles** screen displays all Control Manager user roles. The screen also provides the options for users to create and maintain Control Manager user roles.

User roles define which areas of the Control Manager web console a user can access.

### User Groups
The **User Groups** screen contains Control Manager groups and provides options for creating groups.

Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow administrators to create a group that shares the same access rights.

---

**Note**
Assign users with different access rights and privileges to permit the delegation of certain management tasks without compromising security.
Control Manager User Access with Endpoint Encryption

User Access

Endpoint Encryption user access is similar to Control Manager user access. Administrators can control which parts of the Endpoint Encryption web console users can access (Power User, Operator, or Administrator).

All user accounts created in Control Manager have administrator access to any managed product to which the user has access. This creates a problem if an administrator wants to restrict a user’s access to Power User on the Endpoint Encryption server while allowing access to Control Manager.

MCP Heartbeat

To monitor the status of managed products, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the managed product and to check for commands to the managed product from Control Manager. The Control Manager web console then presents the product status. This means that the managed product’s status is not a real-time, moment-by-moment reflection of the network’s status. Control Manager checks the status of each managed product in a sequential manner in the background. Control Manager changes the status of managed products to offline when a fixed period of time elapses without a heartbeat from the managed product.

Active heartbeats are not the only means Control Manager determines the status of managed products. The following also provide Control Manager with the managed product’s status:

- Control Manager receives logs from the managed product. Once Control Manager receives any type of log from the managed product successfully, this implies that the managed product is working fine.

- In two-way communication mode, Control Manager actively sends out a notification message to trigger the managed product to retrieve the pending command. If server connects to the managed product successfully, it also indicates that the product is working fine and this event counts as a heartbeat.

- In one-way communication mode, the MCP agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.
The MCP heartbeats implement in the following ways:

- **UDP**: If the product can reach the server using UDP, this is the lightest weight, fastest solution available. However, this does not work in NAT or firewall environments. In addition, the transmitting client cannot verify that the server does indeed receive the request.

- **HTTP/HTTPS**: To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat.

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the managed product applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains managed product activity information to display on the console.

### Using the Schedule Bar

Use the schedule bar on the **Agent Communication Schedule** screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

The slots with clock icons denote working status or the hours that the Agent/Communicator sends information to the Control Manager server. White slots indicate idle time. Define working or idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

![Schedule Bar](image)

**Figure A-1. Schedule bar**

The active periods specified by the bar are from 0:00 to 7:00, 8:00 to 4:00 PM, and from 6:00 P.M. to midnight.
Setting an Agent Communication Schedule for a Managed Product

Procedure

1. Open the Control Manager console.

2. Navigate to Administration > Settings > Agent Communication Schedule.

   The Agent Communication Schedule screen appears.

3. Select the managed product schedule to modify.

   The Set Communicator Schedule screen appears.

4. Define the schedule. Specify a new time or use the default setting:
   • To specify a new setting, change the appropriate time slots in the schedule bar and then click Save
   • To use the default setting, return to the Agent Communication Schedule screen. Select the schedule to apply and click Reset to Default Schedule
Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest managed product status information and the need to manage system resources. The default setting is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

Table A-4. Heartbeat Recommendations

<table>
<thead>
<tr>
<th>Heartbeat Frequency</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long-interval Heartbeats (above 60 minutes)</td>
<td>The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status in the Control Manager web console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).</td>
</tr>
<tr>
<td>Short-interval Heartbeats (below 60 minutes)</td>
<td>Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.</td>
</tr>
</tbody>
</table>

Configuring the Agent Communicator Heartbeat

Use the Communication Time-out screen to define the frequency and maximum delay times (in minutes) for the Control Manager server and agent communication.

Note

The agent/communicator heartbeat setting only applies to Communicators for managed products directly controlled by the Control Manager server. Child Control Manager server agent/communicators use pre-defined values:

- **Frequency**: 3 minutes
- **Maximum delay**: 5 minutes
Introducing Trend Micro Control Manager

Procedure

1. Open the Control Manager console.


3. On the working area, leave the default values or specify new settings for the following:
   • **Report managed product status every**: Defines how often the managed product responds to Control Manager server messages. Valid values are between 5 to 480 minutes
   • **If no communication, set status as abnormal after**: Specifies how long Control Manager waits for a response from the managed product before changing its web console status to (inactive). Valid values are between 15 and 1440 minutes.

   **Note**

   The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

4. Click **Save**.

Understanding the Product Directory

A managed product is a representation of an antivirus, content security, or web protection product in the Product Directory. Managed products display as icons (for
example, ( ) or ( )) in the Control Manager web console Product Directory section. These icons represent Trend Micro antivirus, content security, and web protection products. Control Manager supports dynamic icons, which change with the status of the managed product. See your managed product’s documentation for more information on the icons and associated statuses for your managed product.

Indirectly administer the managed products either individually or by groups through the Product Directory. The following table lists the menu items and buttons on the Product Directory screen.

**TABLE A-5. Product Directory Options**

<table>
<thead>
<tr>
<th><strong>Menu Item</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Search</td>
<td>Click this menu item to specify search criteria to perform a search for one or more managed products.</td>
</tr>
<tr>
<td>Configure</td>
<td>After selecting a managed product/directory, move the cursor over this menu item and select a task, to log on to a web-based console using SSO or to configure a managed product.</td>
</tr>
<tr>
<td>Tasks</td>
<td>After selecting a managed product/directory, move the cursor over this menu item and select a task, to perform a specific function (such as deploying the latest components) to a specific managed product or child server or groups of managed products or child servers. Initiate a task from a directory and Control Manager sends requests to all managed products belonging to that directory.</td>
</tr>
<tr>
<td>Directory Management</td>
<td>Click this button to open the Directory Management screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.</td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
</tr>
</tbody>
</table>
Introducing Trend Micro Control Manager

<table>
<thead>
<tr>
<th><strong>Menu Item</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Click this button, after typing a managed product's name, to perform a search for the specified managed product.</td>
</tr>
<tr>
<td>Status</td>
<td>Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.</td>
</tr>
<tr>
<td>Folder</td>
<td>Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product endpoints found in the directory.</td>
</tr>
</tbody>
</table>

**Note**

Managed products belonging to child Control Manager servers cannot have tasks issued to them by the parent Control Manager server.

**Product Directory Structure Recommendations**

Trend Micro recommends the following when planning your Product Directory structure for managed products and child servers:

**Table A-6. Considerations when Grouping Managed Products or Child Servers**

<table>
<thead>
<tr>
<th><strong>Structure</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Company network and security policies</td>
<td>If different access and sharing rights apply to the company network, group managed products and child servers according to company network and security policies.</td>
</tr>
<tr>
<td>Organization and function</td>
<td>Group managed products and child servers according to the company's organizational and functional division. For example, have two Control Manager servers that manage the production and testing groups.</td>
</tr>
</tbody>
</table>
## Structure and Description

<table>
<thead>
<tr>
<th>Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical location</td>
<td>Use geographical location as a grouping criterion if the location of the managed products and child servers affects the communication between the Control Manager server and its managed products or child servers.</td>
</tr>
<tr>
<td>Administrative responsibility</td>
<td>Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.</td>
</tr>
</tbody>
</table>

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

- Configuring managed products
- Request products to perform a Scan Now (if this command is supported)
- View product information, as well as details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on)
- View product-level logs
- Deploy virus pattern, scan engine, anti-spam rule, and program updates

Plan this structure carefully, because the structure also affects the following:

**Table A-7. Considerations for the Structure**

<table>
<thead>
<tr>
<th>Consider</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access</td>
<td>When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire directory. Granting access to a specific managed product only grants access to that specific product.</td>
</tr>
</tbody>
</table>
Introducing Trend Micro Control Manager

**Deployment planning**

<table>
<thead>
<tr>
<th>Consider</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment planning</td>
<td>Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td>
</tr>
<tr>
<td>Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments</td>
<td>OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.</td>
</tr>
</tbody>
</table>

A sample Product Directory appears below:
Managed products identify the registered antivirus or content security product, as well as provide the connection status.

**Note**
All newly registered managed products usually appear in the New Entity folder regardless of the agent type.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="EMAN.png" alt="EMAN" /></td>
<td>InterScan eManager</td>
</tr>
<tr>
<td><img src="OSCE.png" alt="OSCE" /></td>
<td>OfficeScan Corporate Edition</td>
</tr>
<tr>
<td><img src="SPIN.png" alt="SPIN" /></td>
<td>ServerProtect Information Server</td>
</tr>
<tr>
<td><img src="SPNG.png" alt="SPNG" /></td>
<td>ServerProtect Domain</td>
</tr>
<tr>
<td><img src="SPWT.png" alt="SPWT" /></td>
<td>ServerProtect for Windows (Normal Server)</td>
</tr>
</tbody>
</table>
Arrange the Product Directory using the Directory Manager. Use descriptive folder names to group your managed products according to their protection type or the Control Manager network administration model.

### Accessing the Product Directory

Use the Product Directory to administer managed products registered to the Control Manager server.

**Note**

Viewing and accessing the folders in the Product Directory depends on the Account Type and user account access rights.

**Procedure**

- Click **Products** from the main menu.
Manually Deploying Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. Use this method of updating components during virus outbreaks.

Download new components before deploying updates to a specific managed product or groups of managed products.

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.

2. Select a managed product or directory from the Product Directory.
   
   The managed product or directory highlights.

3. Move the cursor over **Tasks** from the Product Directory menu.
4. Select **Deploy <component>** from the drop-down menu.
5. Click **Deploy Now** to start the manual deployment of new components.
6. Monitor the progress through the **Command Tracking** screen.
7. Click the Command Details link on the **Command Tracking** screen to view details for the Deploy Now task.

---

**Viewing Status Summaries for Managed Products**

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

There are two ways to view the managed products status summary:

- Through the dashboard using the Threat Detection Results widget (found on the Summary tab)
- Through the Product Directory

**Accessing Through the Dashboard**

**Procedure**

- Upon opening the Control Manager web console, the **Summary** tab on the Dashboard displays the summary of the entire Control Manager network. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

**Accessing Through the Product Directory**

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.
2. From the Product Directory tree, select the desired folder or managed product.
   • If you click a managed product, the Product Status tab displays the managed product's summary.
   • If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries.

Note
By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last Month in the Display summary for list.

Configuring Managed Products

Depending on the product and agent version you can configure the managed product from the managed product’s web console or through a Control Manager-generated console.

Procedure
1. Click Products on the main menu.
   The Product Directory screen appears.
2. Select the desired managed product from the Product Directory tree.
   The product status appears in the right-hand area of the screen.
3. Move the cursor over Configure in the Product Directory menu.
4. Select one of the following:
   • Configuration Replication: The Configuration Settings screen appears.
     a. Select the folder to which the selected managed product’s settings replicate from the Product Directory tree.
     b. Click Replicate.
The selected managed product’s settings replicate to the target managed products.

- **<Managed Product Name> Single Sign On**: The managed product’s web console or Control Manager-generated console appears.
  a. Configure the managed product from the web console.

---

**Note**

For additional information about configuring managed products, refer to the managed product's documentation.

---

**Issuing Tasks to Managed Products**

Use the Tasks menu item to invoke available actions to a specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable or disable Real-time Scan
- Start Scan Now

Deploy the latest spam rule, pattern, or scan engine to managed products with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

---

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.

2. Select the managed product or directory to issue a task.
3. Move the cursor over **Tasks**.

4. Click a task from the list. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

---

**Querying and Viewing Managed Product Logs**

Use the Logs tab to query and view logs for a group or a specific managed product.

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.

2. Select the desired managed product or folder from the Product Directory.

3. Move the cursor over **Logs** in the Product Directory menu.

4. Click **Logs** from the drop-down menu.

   The **Ad Hoc Query > Step 2: Select Data View** screen appears.

5. Specify the data view for the log:
   
a. Select the data to query from the Available Data Views area.

b. Click **Next**.
Introducing Trend Micro Control Manager

The Ad Hoc Query > Step 3: Query Criteria screen appears.

6. Specify the data to appear in the log and the order in which the data appears. Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.
   a. Click Change column display.

   The Select Display Sequence screen appears.

   b. Select a query column from the Available Fields list. Select multiple items using the Shift or Ctrl keys.

   c. Click > to add items to the Selected Fields list.
d. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

e. Click **Back** when the sequence fits your requirements.

7. Specify the filtering criteria for the data:

   ![Note]
   *When querying for summary data, users must specify the items under Required criteria.*

   - **Required criteria:**
     - Specify a Summary Time for the data or whether you want COOKIES to appear in your reports.
   
   - **Custom criteria:**
     a. Specify the criteria filtering rules for the data categories:
       - **All of the criteria:** This selection acts as a logical AND function. Data appearing in the report must meet all the filtering criteria.
       
       - **Any of the criteria:** This selection acts as a logical OR function. Data appearing in the report must meet any of the filtering criteria.

     b. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

   ![Tip]
   *If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.*

8. Save the query:

   a. Click **Save this query to the saved Ad Hoc Queries list**.

   b. Type a name for the saved query in the **Query Name** field.
9. Click **Query**.

The **Results** screen appears.

10. Save the report as a CSV file:
    a. Click **Export to CSV**.
    b. Click **Download**.
    c. Specify the location to save the file.
    d. Click **Save**.

11. Save the report as an XML file:
    a. Click **Export to XML**.
    b. Click **Download**.
    c. Specify the location to save the file.
    d. Click **Save**.

**Tip**

To query more results on a single screen, select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

12. Save the settings for the query:
    a. Click **Save query settings**.
    b. Type a name for the saved query in the **Query Name** field.
    c. Click **OK**.

        The saved query appears on the **Saved Ad Hoc Queries** screen.
About Recovering Managed Products Removed From the Product Directory

The following scenarios can cause Control Manager to delete managed products from the Product Directory:

- Reinstalling the Control Manager server and selecting **Delete existing records and create a new database**
  
  This option creates a new database using the name of the existing one.

- Replacing the corrupted Control Manager database with another database of the same name

- Accidentally deleting the managed product from Directory Management

If the records for a Control Manager server's managed products are lost, TMI agents on the products still "know" where they are registered. The Control Manager agent automatically re-registers itself after 8 hours or when the service restarts.

MCP agents do not re-register automatically. Administrators must manually re-register managed products using MCP agents.

Recovering Managed Products Removed From the Product Directory

**Procedure**

- Restart the Trend Micro Control Manager service on the managed product server. For more information, see *Stopping and Restarting Control Manager Services on page A-31*.

- Wait for the Agent to re-register itself: By default, the older Control Manager agents verify their connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

- Manually re-register to Control Manager: MCP agents do not re-register automatically and need to be manually re-registered to the Control Manager server.
Stopping and Restarting Control Manager Services

Use the Windows Services screen to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager

**Note**

These are the services that run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

**Procedure**

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the Services screen.
2. Right-click <Control Manager service>, and then click **Stop**.
3. Right-click <Control Manager service>, and then click **Start**.

Searching for Managed Products, Product Directory Folders, or Computers

Use the Search button to quickly locate a specific managed product in the Product Directory.

Searching for a Folder or Managed Product

**Procedure**

1. Access the Product Directory.
2. Type the display name of the managed product in the **Find entity** field.

3. Click **Search**.

---

**Performing an Advanced Search**

**Procedure**

1. Access the Product Directory.

2. Click **Advanced Search**.

   The **Advanced Search** screen appears.

3. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.

4. Click **Search** to start searching.

   Search results appear in the **Search Result** folder of the Product Directory.

---

**Refreshing the Product Directory**

**Procedure**

- On the **Product Directory** screen, click the **Refresh** icon on the upper right corner of the screen.
Understanding the Directory Management Screen

After registering to Control Manager, the managed product appears in the Product Directory under the default folder.

Use the Directory Management screen to customize the Product Directory organization to suit your administration needs. For example, you can group products by location or product type (messaging security, web security, file storage protection).

The directory allows you to create, modify, or delete folders, and move managed products between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the managed products belonging to each folder. Consider the following factors when planning and implementing your folder and managed product structure:

- Product Directory
- User Accounts
- Deployment Plans
- Ad Hoc Query
- Control Manager reports

Group managed products according to geographical, administrative, or product-specific reasons. In combination with different access rights used to access managed products or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages.

**Table A-9. Product Grouping Comparison**

<table>
<thead>
<tr>
<th>Grouping Type</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical or Administrative</td>
<td>Clear structure</td>
<td>No group configuration for identical products</td>
</tr>
<tr>
<td>Product type</td>
<td>Group configuration and status is available</td>
<td>Access rights may not match</td>
</tr>
<tr>
<td>GROUPING TYPE</td>
<td>ADVANTAGES</td>
<td>DISADVANTAGES</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Combination of both</td>
<td>Group configuration and access right management</td>
<td>Complex structure, may not be easy to manage</td>
</tr>
</tbody>
</table>

**Using the Directory Management Screen Options**

Use these options to manipulate and organize managed products in your Control Manager network.

The **Directory Management** screen provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products or directories in the Product Directory
- Remove managed products or directories from the Product Directory

---

**Note**

The keep permissions check box allows a folder to keep its source permission when moved.

---

**Using the Directory Management Screen**

**Procedure**

- Select a managed product or directory and click **Rename** to rename a managed product or directory
- Click + or the folder to display the managed products belonging to a folder
- Drag managed products or directories to move the managed products or directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory
Accessing the Directory Management Screen

Use the **Directory Management** screen to group managed products together.

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.
   
   The **Directory Management** screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

**Procedure**

1. Click **Products** from the main menu.
   
   The **Product Directory** screen appears.
2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select **Local Folder**.

4. Click **Add Folder**.

   The **Add Directory** screen appears.

5. Type a name for the new directory in the **Directory name** field.

6. Click **Save**.

---

**Note**

Except for the **New Entity** folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (, ), *, +, -, comma, period, +, ?, @, [, ], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabetic characters (a/A to z/Z).

---

**Renaming Folders or Managed Products**

Rename directories and managed products on the **Directory Management** screen.

---

**Note**

Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

---

**Procedure**

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to rename.
4. Click Rename.

The Rename Directory screen appears.

5. Type a name for the managed product or directory in the Directory name field.

6. Click Save.

7. Click OK.

The managed product or directory displays in the Product Directory with the new name.

---

**Moving Folders or Managed Products**

When moving folders pay special attention to the Keep the current user access permissions when moving managed products/folders check box. If you select this check box and move a managed product or folder, the managed product or folder keeps the permissions from its source folder. If you clear the keep permissions check box, and then move a managed product or folder, the managed product or folder assumes the access permissions from its new parent folder.

---

**Procedure**

1. Click Products from the main menu.

   The Product Directory screen appears.

2. Click Directory Management from the Product Directory menu.

   The Directory Management screen appears.

3. On the working area, select the folder or managed product to move.

4. Drag the folder or managed product to the target new location.

5. Click Save.
Deleting User-Defined Folders

Take caution when deleting user-defined folders on the Directory Management screen. You may accidentally delete a managed product which causes it to unregister from the Control Manager server.

**Note**

You cannot delete the New Entity folder.

**Procedure**

1. Click Products from the main menu.
   
   The Product Directory screen appears.

2. Click Directory Management from the Product Directory menu.
   
   The Directory Management screen appears.

3. Select the managed product or directory to delete.

4. Click Delete.
   
   A confirmation dialog box appears.

5. Click OK.

6. Click Save.

Downloading and Deploying New Components

Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats.

By default, Control Manager enables download only on components belonging to managed products registered to the Control Manager server. Control Manager enables virus pattern download even if no managed products are registered to the Control Manager server.
The following are the components to update (listed according to the frequency of recommended update).

**TABLE A-10. Available Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern files/Cleanup templates</td>
<td>Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections</td>
</tr>
<tr>
<td>Antispam rules</td>
<td>Antispam rules are the Trend Micro-provided files used for antispam and content filtering</td>
</tr>
<tr>
<td>Engines</td>
<td>Engines refer to virus/malware scan engines, Damage Cleanup engine, VirusWall engines, the Spyware/Grayware engine and so on. These components perform the actual scanning and cleaning functions.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OfficeScan Plug-in Programs</td>
<td>OfficeScan Plug-in Programs (for example, Trend Micro Security for Mac).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The OfficeScan web console displays all available Plug-in Programs. You can specify to download any of them from Control Manager. However, Control Manager may not have the downloaded the Plug-in Program. Which means that OfficeScan cannot download the specified Plug-in Program from Control Manager. Before specifying a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.</td>
</tr>
<tr>
<td>Product programs and widget pool</td>
<td>Product-specific components (for example, Service Pack releases) and the Control Manager widget pool</td>
</tr>
</tbody>
</table>

**Note**

Only registered users are eligible for components update.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

The **Component List** screen presents a full list of all components that Control Manager has available for managed products. The list also matches components with managed
Introducing Trend Micro Control Manager

products that use the component. Click **Updates > Component List** to open the **Component List** screen.

![Component List screenshot](image)

**FIGURE A-2. The Component List screen**

The Control Manager server only retains the latest component version. You can trace a component's version history by viewing `root>:\Program Files\Trend Micro \Control Manager\AU_log\TmuDump.txt` entries. `TmuDump.txt` generates when ActiveUpdate debugging is enabled.

---

**Tip**

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed products or services. When you register managed products or activate services at a later time, be sure to configure the manual or scheduled download of applicable components.

---

**Manually Downloading Components**

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Trend Micro recommends the following method to configure manual downloads. Manually downloading components requires multiple steps:
Tip
Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

- Step 1: Configure a deployment plan for your components
- Step 2: Configure your proxy settings, if you use a proxy server
- Step 3: Select the components to update
- Step 4: Configure the download settings
- Step 5: Configure the automatic deployment settings
- Step 6: Complete the manual download

Step 1: Configure a Deployment Plan for Your Components

Procedure

1. Navigate to Updates > Deployment Plan.

   The Deployment Plan screen appears.

2. Click Add.

   The Add New Plan screen appears.
3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

The **Add New Schedule** screen appears.

5. On the **Add New Schedule** screen, choose a deployment time schedule by selecting one the following options:
   - **Start at**: Performs the deployment at a specific time.
     Use the menus to designate the time in hours and minutes.
   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.
     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the **Product Directory** folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.
The **Add New Plan** screen appears.

8. Click **Save** to apply the new deployment plan.

---

**Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)**

**Procedure**

1. Navigate to **Administration > Settings > Proxy Settings**.

   The **Connection Settings** screen appears.

[![Connection Settings Screen](image.png)]

2. Select **Use a proxy server for pattern, engine, and license updates**.

3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Type the host name or IP address of the server in the **Server name or IP address** field.

5. Type a port number in the **Port** field.

6. Type a log on name and password if your server requires authentication.
7. Click **Save**.

---

**Step 3: Select the Components to Update**

**Procedure**

1. **Navigate to Updates > Manual Download.**

   The **Manual Download** screen appears.

   ![Manual Download screen](image)

   - From the **Component Category** area select the components to download.
   
   a. Click the + icon to expand the component list for each component group.
   
   b. Select the components to download. To select all components for a group, select:
Step 4: Configure the Download Settings

Procedure

1. Select the update source:
   - **Internet: Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source**: Type the URL of the update source in the accompanying field.

     After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   **Tip**

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.
Step 5: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:
   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy to all products immediately**: Components download to Control Manager, and then deploy to managed products
   - **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found**: Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

   **Tip**

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

Step 6: Complete the Manual Download

Procedure

1. Click **Download Now** and then click **OK** to confirm.
   The download response screen appears. The progress bar displays the download status.

2. Click **Command Details** to view details from the **Command Details** screen.
3. Click **OK** to return to the **Manual Download** screen.

### Understanding Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

---

**Note**

Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

**Example:** The administrator decides that they do not want Control Manager to download components on weekends or after working hours throughout the week. The administrator enables **Daily Schedule Exception** and selects **Saturday** and **Sunday**. The administrator then enables **Hourly Schedule Exception** and specifies the hours of **00:00 to 9:00** and **18:00 to 24:00**.

---

### Configuring Scheduled Download Exceptions

**Procedure**

1. Navigate to **Updates > Scheduled Download Exceptions**.

   The **Scheduled Download Exceptions** screen appears.
2. Do one or more of the following:
   - To schedule a daily exception, under Daily Schedule Exception, select the day(s) to prevent downloads, and then select **Do not download updates on the specified day(s)**. Every week, Control Manager blocks all downloads during the selected day(s).
   - To schedule an hourly exception, under Hourly Schedule Exception, select the hour(s) to prevent downloads, and then select **Do not download updates on the specified hour(s)**. Every day, Control Manager blocks all downloads during the selected hours.

3. Click **Save**.

### Configuring Scheduled Downloads

Configure scheduled downloading of components to keep your components up to date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling a download for a component group downloads all components in the group.

Use the **Scheduled Download** screen to obtain the following information for components currently in your Control Manager system:

- **Frequency**: Shows how often the component updates
- **Enabled**: Indicates if the schedule for the component is enabled or disabled
• **Update Source**: Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

• Step 1: Configure a Deployment Plan for your components
• Step 2: Configure your proxy settings, if you use a proxy server
• Step 3: Select the components to update
• Step 4: Configure the download schedule
• Step 5: Configure the download settings
• Step 6: Configure the automatic deployment settings
• Step 7: Enable the schedule and save settings

**Step 1: Configure a Deployment Plan for Your Components**

**Procedure**

1. Navigate to **Updates > Deployment Plan**.
   
The **Deployment Plan** screen appears.

2. Click **Add**.
   
The **Add New Plan** screen appears.
3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. Choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.
     
     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.
     
     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

**Procedure**

1. Navigate to **Administration > Settings > Proxy Settings**.

   The **Connection Settings** screen appears.

   ![Proxy Settings Screen](image)

2. Select **Use a proxy server for pattern, engine, and license updates**.

3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Type the host name or IP address of the server in the **Server name or IP address** field.

5. Type a port number for the proxy server in the **Port** field.

6. Type a logon name and password if your server requires authentication.
7. Click **Save**.

---

**Step 3: Select the Components to Update**

**Procedure**

1. Navigate to **Updates > Scheduled Download**.

   The **Scheduled Download** screen appears.

   ![Scheduled Download Screen]

2. From the Component Category area select the components to download.
   
a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

   - **All Pattern files/Cleanup templates**
   - **All Antispam rules**
   - **All Engines**
   - **OfficeScan Plug-in Programs**
   - **Product programs and widget pool**

   The `<Component Name>` screen appears. Where `<Component Name>` represents the name of the selected component.
Step 4: Configure the Download Schedule

Procedure

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.

2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download by minutes, hours, days, or weeks.

3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.
Step 5: Configure the Download Settings

Procedure

1. Select the update source:
   
   - **Internet: Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.
   
   - **Other update source**: Type the URL of the update source in the accompanying field.

   After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   **Note**
   
   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 6: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:

   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     
     - Deploying to the managed products individually
• Testing the updated components before deployment

• **Deploy immediately:** Components download to Control Manager, then deploy to managed products

• **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select

• **When new updates found:** Components download to Control Manager, and deploy to managed products when new components are available from the update source

---

**Note**

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save**, your settings will be lost.

---

2. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.

3. Click **Save**.

---

### Step 7: Enable the Schedule and Save Settings

**Procedure**

1. Click the status button in the **Enable** column.

2. Click **Save**.

---

### Configuring Scheduled Download Schedule and Frequency

Specify how often Control Manager obtains component updates at the Schedule and Frequency group.

**Procedure**

1. Navigate to **Updates > Scheduled Download**.
Introducing Trend Micro Control Manager

The Scheduled Download screen appears.

2. From the Component Category area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the components to download. To select all components for a group, select:
      • All Pattern files/Cleanup templates
      • All Antispam rules
      • All Engines
      • OfficeScan Plug-in Programs
      • Product programs and widget pool

      The Component Name> screen appears. Where Component Name> is the name of the component you selected.

3. Under Schedule and frequency:
   a. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minutes, hours, days, or weeks.
   b. Use the Start time drop-down menus to specify the date and time the schedule starts to take effect.

4. Click Save.

Configuring Scheduled Download Settings

The Download Settings group defines the components Control Manager automatically downloads and the download method.

Procedure

1. Navigate to Updates > Scheduled Download.
The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the components to download. To select all components for a group, select:
      - All Pattern files/Cleanup templates
      - All Antispam rules
      - All Engines
      - OfficeScan Plug-in Programs
      - Product programs and widget pool

      The Component Name> screen appears. Where Component Name> represents the name of the selected component.

3. Under Download settings, select one of the following update sources:
   - **Internet: Trend Micro update server**: (default setting) Control Manager downloads the latest components from the Trend Micro ActiveUpdate server
   - **Other update source**: specify the URL of the latest component source, for example, your company's Intranet server

      After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.

4. Select **Retry frequency** to instruct Control Manager to retry downloading latest components. Specify the number of attempts and the frequency of each set of attempts in the appropriate fields.

---

**Note**

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.
5. If you are using a proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings from the **Connection Settings** screen.

6. Click **Save**.

---

### Configuring Scheduled Download Automatic Deployment Settings

Use the Automatic deployment settings group to set how Control Manager deploys updates.

**Procedure**

1. Navigate to **Updates > Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

   The Component Name> screen appears. Where Component Name> represents the name of the selected component.

3. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:
• **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
  - Deploying to the managed products individually
  - Testing the updated components before deployment
• **Deploy immediately**: Components download to Control Manager, then deploy to managed products
• **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
• **When new updates found**: Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

---

**Note**

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

4. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.

5. Click **Save**.

---

**Note**

The settings in Automatic deployment settings only apply to components used by managed products.

---

**Understanding Deployment Plans**

A deployment plan allows you to set the order in which Control Manager updates your groups of managed products. With Control Manager, you can implement multiple deployment plans to different managed products at different schedules. For example, during an outbreak involving an email-borne virus, you can prioritize the update of your email message scanning software components such as the latest virus pattern file for Trend Micro ScanMail for Microsoft Exchange.
The Control Manager installation creates two deployment plans:

• Deploy to All Managed Products Now (Default): default plan used during component updates

• Deploy to All Immediately (Outbreak-Prevention): default plan for the Outbreak Prevention Services Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately.

Select or create plans from the Manual and Scheduled download screens. Customize these plans, or create new ones, as required by your network. For example, create deployment plans according to the nature of the outbreak:

• Email-borne virus

• File-sharing virus

Deploying updates to the Product Directory is separate from the download process. Control Manager downloads the components and follows the deployment plan according to manual or scheduled download settings.

When creating or implementing a deployment plan, consider the following points:

• Assign deployment schedules to folders, not to specific products.

Planning the contents of the Product Directory folders, therefore, becomes very important.

• You can only include one folder for each deployment plan schedule.

However, you can specify more than one schedule per deployment plan.

• Control Manager bases the deployment plan delays on the completion time of the download, and these delays are independent of each other.

For example, if you have three folders to update at 5 minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders.
Configuring Proxy Settings

Configure the proxy server connection for component downloads and for license updates.

Procedure

1. Navigate to Administration > Settings > Proxy Settings.

   The Connection Settings screen appears.

2. Select Use a proxy server for pattern, engine, and license updates.

3. Select the protocol:
   - HTTP
   - SOCKS 4
   - SOCKS 5

4. Type the host name or IP address of the server in the Server name or IP address field.

5. Type a port number in the Port field.

6. Type a log on name and password if your server requires authentication.

7. Click Save.
Introducing Trend Micro Control Manager

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (the default download source) or other update source provides a more secure method for retrieving components.

Downloading components from a shared folder in a network requires setting the local Windows and Remote UNC authentications.

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

• Administrator privilege
• Log on as a batch job policy set

The remote UNC authentication feature uses a user account from the component source server that has permission to share a folder to which Control Manager will download updates.

Enabling HTTPS Download

Procedure

1. Navigate to Updates > Update/Deployment Settings. The Update/Deployment Settings screen appears.

2. Select Enable HTTPS for the default update download source.
3. Click Save.


5. On the working area under Download settings, select Internet: Trend Micro update server or specify your organization's component source server in the Other update source field.

6. Click Save.

Enabling UNC Download

Procedure

1. Navigate to Updates > Update/Deployment Settings.

   The Update/Deployment Settings screen appears.

2. Type the Local Windows Authentication and Remote UNC Authentication user names and passwords.

3. Click Save.


5. On the working area under Download settings, select Other update source and then specify the shared network folder.

6. Click Save.

Setting "Log on as batch job" Policy

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

- Administrator privilege
- "Log on as a batch job" policy set
Introducing Trend Micro Control Manager

**Procedure**

1. Click Start > Settings > Control Panel.
2. Click Administrative Tools.
4. Click Local Policies > User Rights Assignment.
5. Double-click Log on as a batch job.
   
   The Log on as a batch job Properties dialog box appears.
6. Add the user if they do not appear on the list.

**Using Logs**

Although Control Manager receives data from various log types, Control Manager allows users to query the log data directly from the Control Manager database. Users can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

**Understanding Managed Product Logs**

Managed product logs contain information about the performance of your managed products. You can obtain information for specific products or groups of products administered by the parent or child server. With Control Manager’s data query on logs and data filtering capabilities, administrators can focus on the information they need.
More logs mean abundant information about the Control Manager network. However, these logs occupy disk space. You must balance the need for information with your available system resources.

Managed products generate different kinds of logs depending on their function.

**Table A-11. Managed Product Logs**

<table>
<thead>
<tr>
<th>Log Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Information</td>
<td>Product information logs provide information on subjects ranging from user access and events on managed products to component deployment and update status.</td>
</tr>
<tr>
<td></td>
<td>• Managed Product Information</td>
</tr>
<tr>
<td></td>
<td>• Component Information</td>
</tr>
<tr>
<td>Security Threat Information</td>
<td>Security threat logs provide information on known and potential security threats detected on your network.</td>
</tr>
<tr>
<td></td>
<td>• Virus/Malware Information</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Information</td>
</tr>
<tr>
<td></td>
<td>• Content Violation Information</td>
</tr>
<tr>
<td></td>
<td>• Spam Violation Information</td>
</tr>
<tr>
<td></td>
<td>• Policy/Rule Violation Information</td>
</tr>
<tr>
<td></td>
<td>• Web Violation/Reputation Information</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Information</td>
</tr>
<tr>
<td></td>
<td>• Overall Threat Information</td>
</tr>
<tr>
<td>Data Protection Information</td>
<td>Data Protection logs provide information on DLP incidents, template matches, and incident sources.</td>
</tr>
<tr>
<td></td>
<td>• Data Loss Prevention Information</td>
</tr>
</tbody>
</table>
Querying Log Data

Ad Hoc Queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators.

While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc query consists of the following process:

• Step 1: Select the managed product or current Control Manager server for the query
• Step 2: Select the data view to query
• Step 3: Specify filtering criteria and the specific information that displays
• Step 4: Save and complete the query
• Step 5: Export the data to a CSV or XML file

---

**Note**

Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Saved Ad Hoc Queries** screen.

---

Understanding Data Views

A data view is a table consisting of clusters of related data cells. Data views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager allows direct queries to the Control Manager database. Data views are available to Control Manager 5 report templates and to Ad Hoc Query requests.
Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example, the Virus/Malware Action/Result Summary data view has the following headings:

- Action Result
- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

As a table, a data view takes the following form with potential subheadings under each heading:

**TABLE A-12. Sample Data View**

<table>
<thead>
<tr>
<th>ACTION RESULT</th>
<th>ACTION TAKEN</th>
<th>UNIQUE ENDPOINTS</th>
<th>UNIQUE SOURCES</th>
<th>DETECTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This information is important to remember when specifying how data displays in a report template.

Control Manager separates data views into two major categories: Product Information and Security Threat Information. See the appendix for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

**Understanding Reports**

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduced radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control
Manager 6.0 continues to support report templates from previous Control Manager versions, however Control Manager 6.0 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager categorizes report templates according to the following types:

- Control Manager 5 templates: User-defined customized report templates that use direct database queries (database views) and report template elements (charts and tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions. For more information on Control Manager 5 templates, see Understanding Control Manager 5 Templates on page A-69.

- Control Manager 3 templates: Includes pre-defined templates. For more information on Control Manager 3 templates, see Understanding Control Manager 3 Templates on page A-76.

Understanding Control Manager 5 Templates

Control Manager 5 report templates use database views as the information foundation for reports. For more information on data views, see Understanding Data Views on page A-67. The look and feel of generated reports falls to the report elements. Report elements consist of the following.

Table A-13. Control Manager 5 Report Template Elements

<table>
<thead>
<tr>
<th>Template Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page break</td>
<td>Inserts a page break for a report. Each report page supports up to three report template elements.</td>
</tr>
<tr>
<td>Static text</td>
<td>Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.</td>
</tr>
<tr>
<td>Bar chart</td>
<td>Inserts a bar chart into a report template.</td>
</tr>
<tr>
<td><strong>TEMPLATE ELEMENT</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Line chart</td>
<td>Inserts a line graph into a report template.</td>
</tr>
<tr>
<td>Pie chart</td>
<td>Inserts a pie chart into a report template.</td>
</tr>
<tr>
<td>Dynamic table</td>
<td>Inserts a dynamic table/pivot table into a report template.</td>
</tr>
<tr>
<td>Grid table</td>
<td>Inserts a table into a report template. The information in a grid table will be the same as the information that displays in an Ad Hoc Query.</td>
</tr>
</tbody>
</table>

Each Control Manager 5 template can contain up to 100 report template elements. Each page in the report template can contain up to three report template elements. Use page breaks to create report template pages.

To better understand Control Manager 5 report templates, Trend Micro provides the following pre-defined report templates.

---

**Note**

Access the **Report Templates** screen to view the Trend Micro pre-defined templates.
### TABLE A-14. Control Manager 5 Pre-defined Templates

<table>
<thead>
<tr>
<th>TEMPLATE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| TM-Content Violation Detection Summary | Provides the following information:  
- Content Violation Detection Grouped by Day (Line chart)  
- Policy in Violation Count Grouped by Day (Line chart)  
- Sender/Users in Violation Count Grouped by Day (Line chart)  
- Recipient Count Grouped by Day (Line chart)  
- Top 25 Policies in Violation (Bar chart)  
- Content Violation Policy Summary (Grid table)  
- Top 25 Senders/Users in Violation (Bar chart)  
- Content Violation Senders/Users in Violation Summary (Grid table)  
- Action Result Summary (Pie chart) |
<table>
<thead>
<tr>
<th><strong>TEMPLATE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| TM-Managed Product Connection/Component Status | Provides the following information:  
  - Server/Appliance Connection Status (Pie chart)  
  - Client Connection Status (Pie chart)  
  - Server/Appliance Pattern File/Rule Update Status (Pie chart)  
  - Client Pattern File/Rule Update Status (Pie chart)  
  - Server/Appliance Scan Engine Update Status (Pie chart)  
  - Client Scan Engine Update Status (Pie chart)  
  - Pattern File/Rule Summary for Servers/Appliances (Grid table)  
  - Pattern File/Rule Summary for Clients (Grid table)  
  - Scan Engine Summary for Servers/Appliances (Grid table)  
  - Scan Engine Summary for Clients (Grid table) |
| TM-Overall Threat Summary       | Provides the following information:  
  - Complete Network Security Risk Analysis Summary (Grid table)  
  - Network Protection Boundary Summary (Grid table)  
  - Security Risk Entry Point Analysis Information (Grid table)  
  - Security Risk Destination Analysis Information (Grid table)  
  - Security Risk Source Analysis Information (Grid table) |
<table>
<thead>
<tr>
<th>TEMPLATE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TM-Spam Detection Summary</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Spam Detection Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Recipient Domain Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Recipient Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Recipient Domains (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Overall Spam Violation Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Spam Recipients (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Spam Recipient Summary (Grid table)</td>
</tr>
<tr>
<td>TM-Spyware/Grayware Detection Summary</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Detection Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Unique Spyware/Grayware Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Source Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Destination Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Spyware/Grayware (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Overall Spyware/Grayware Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Spyware/Grayware Sources (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Source Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Spyware/Grayware Destinations (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Destination Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Action Result Summary (Pie Chart)</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware Action/Result Summary (Grid table)</td>
</tr>
</tbody>
</table>
### Template: TM-Suspicious Threat Detection Summary

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Detection Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Rule in Violation Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Sender Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Recipient Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Source IP Address Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Destination IP Address Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Senders (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Recipients (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Sender Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Riskiest Recipient Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Source IP Addresses (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Destination IP Addresses (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Source Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Riskiest Destination Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Protocol Names (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Suspicious Threat Protocol Detection Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Overall Suspicious Threat Summary (Grid table)</td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TM-Virus/Malware Detection Summary</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Virus/Malware Detection Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Unique Virus/Malware Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Infection Destination Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Virus/Malware (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Overall Virus/Malware Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Infection Sources (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Virus/Malware Infection Source Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Infection Destinations (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Virus/Malware Infection Destination Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Action Result Summary (Pie chart)</td>
</tr>
<tr>
<td></td>
<td>• Virus/Malware Action/Result Summary (Grid table)</td>
</tr>
<tr>
<td>TM-Web Violation Detection Summary</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td></td>
<td>• Web Violation Detection Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Policy in Violation Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Client in Violation Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• URL in Violation Count Grouped by Day (Line chart)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Policies in Violation (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Overall Web Violation Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 Clients in Violation (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Web Violation Client IP Address Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Top 25 URLs in Violation (Bar chart)</td>
</tr>
<tr>
<td></td>
<td>• Web Violation URL Summary (Grid table)</td>
</tr>
<tr>
<td></td>
<td>• Filter/Blocking Type Summary (Pie chart)</td>
</tr>
</tbody>
</table>
Understanding Control Manager 3 Templates

Control Manager added 87 pre-generated report templates divided into six categories: Executive Summary, Gateway, Mail Server, Server, Desktop, Network Products, and Data Loss Prevention.

---

**Note**

In Control Manager 3.5, spyware/grayware were no longer considered viruses. This change affects the virus count in all original virus-related reports.

---

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the View link adjacent to the report becomes available.

Use the Report Category list on the Control Manager screen to peruse the six categories of reports listed below:

**Table A-15. Executive Summary Reports and Report Types**

<table>
<thead>
<tr>
<th>Executive Summary Reports</th>
<th>Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware/Grayware Detection Reports</td>
<td>• Spyware/Grayware detected</td>
</tr>
<tr>
<td></td>
<td>• Most commonly detected Spyware/Grayware (10, 25, 50, 100)</td>
</tr>
<tr>
<td></td>
<td>• Detected Spyware/Grayware list for all entities</td>
</tr>
<tr>
<td>Virus Detection Reports</td>
<td>• Viruses detected</td>
</tr>
<tr>
<td></td>
<td>• Most commonly detected viruses (10, 25, 50, 100)</td>
</tr>
<tr>
<td></td>
<td>• Virus infection list for all entities</td>
</tr>
</tbody>
</table>
### Executive Summary Reports

<table>
<thead>
<tr>
<th>Executive Summary Reports</th>
<th>Report Types</th>
</tr>
</thead>
</table>
| Comparative Reports      | • Spyware/Grayware, grouped by (Day, Week, Month)  
                           | • Viruses, grouped by (Day, Week, Month)   
                           | • Damage cleanups, grouped by (Day, Week, Month)  
                           | • Spam, grouped by (Day, Week, Month) |
| Vulnerability Reports    | • Machine risk level assessment  
                           | • Vulnerability assessment  
                           | • Most commonly cleaned infections (10, 25, 50, 100)  
                           | • Worst damage potential vulnerabilities (10, 25, 50, 100)  
                           | • Vulnerabilities ranked by risk level |

### Table A-16. Gateway Product Reports and Report Types

<table>
<thead>
<tr>
<th>Gateway Product Reports</th>
<th>Report Types</th>
</tr>
</thead>
</table>
| Spyware/Grayware Detection Reports | • Spyware/Grayware detected  
                                 | • Most commonly detected Spyware/Grayware (10, 25, 50, 100) |
| Virus Detection Reports | • Viruses detected  
                          | • Most commonly detected viruses (10, 25, 50, 100) |
| Comparative Reports     | • Spyware/Grayware, grouped by (Day, Week, Month)  
                           | • Spam, grouped by (Day, Week, Month)  
<pre><code>                       | • Viruses, grouped by (Day, Week, Month) |
</code></pre>
<table>
<thead>
<tr>
<th><strong>GATEWAY PRODUCT REPORTS</strong></th>
<th><strong>REPORT TYPES</strong></th>
</tr>
</thead>
</table>
| Deployment Rate Reports     | • Detailed summary  
|                             | • Basic summary  
|                             | • Detailed failure rate summary  
|                             | • OPS deployment rate for IMSS |

**TABLE A-17. Mail Server Product Reports and Report Types**

<table>
<thead>
<tr>
<th><strong>MAIL SERVER PRODUCT REPORTS</strong></th>
<th><strong>REPORT TYPES</strong></th>
</tr>
</thead>
</table>
| Spyware/Grayware Detection Reports | • Spyware/Grayware detected  
|                                  | • Most commonly detected Spyware/Grayware (10, 25, 50, 100) |
| Virus Detection Reports         | • Viruses detected  
|                                  | • Top senders of infected email (10, 25, 50, 100)  
|                                  | • Most commonly detected viruses (10, 25, 50, 100) |
| Comparative Reports             | • Spyware/Grayware, grouped by (Day, Week, Month)  
|                                  | • Viruses, grouped by (Day, Week, Month) |
| Deployment Rate Reports         | • Detailed summary  
|                                  | • Basic summary  
|                                  | • Detailed failure rate summary |

**TABLE A-18. Server Based Product Reports and Report Types**

<table>
<thead>
<tr>
<th><strong>SERVER BASED PRODUCT REPORTS</strong></th>
<th><strong>REPORT TYPES</strong></th>
</tr>
</thead>
</table>
| Spyware/Grayware Detection Reports | • Spyware/Grayware detected  
|                                  | • Most commonly detected Spyware/Grayware (10, 25, 50, 100) |
## Table A-19. Desktop Product Reports and Report Types

<table>
<thead>
<tr>
<th>Desktop Product Reports</th>
<th>Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware/Grayware Detection Reports</td>
<td>Spyware/Grayware detected</td>
</tr>
<tr>
<td></td>
<td>Most commonly detected Spyware/Grayware (10, 25, 50, 100)</td>
</tr>
<tr>
<td>Virus Detection Reports</td>
<td>Viruses detected</td>
</tr>
<tr>
<td></td>
<td>Most commonly detected viruses (10, 25, 50, 100)</td>
</tr>
<tr>
<td>OfficeScan Client Information Reports</td>
<td>Detailed summary</td>
</tr>
<tr>
<td></td>
<td>Basic summary</td>
</tr>
<tr>
<td>OfficeScan Product Registration Report</td>
<td>Registration status</td>
</tr>
<tr>
<td>Comparative Reports</td>
<td>Spyware/Grayware, grouped by (Day, Week, Month)</td>
</tr>
<tr>
<td></td>
<td>Viruses, grouped by (Day, Week, Month)</td>
</tr>
</tbody>
</table>
### DeskTop Product Reports and Report Types

<table>
<thead>
<tr>
<th>DeskTop Product Reports</th>
<th>Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>OfficeScan Server Deployment Reports</td>
<td>• Detailed summary&lt;br&gt;• Basic summary&lt;br&gt;• Detailed failure rates summary</td>
</tr>
<tr>
<td>OfficeScan Damage Cleanup Services Reports</td>
<td>• Detailed summary&lt;br&gt;• Most commonly cleaned infections (10, 25, 50, 100)</td>
</tr>
</tbody>
</table>

#### Table A-20. Network Product Reports and Report Types

<table>
<thead>
<tr>
<th>Network Product Reports</th>
<th>Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network VirusWall Reports</td>
<td>• Policy violation report, grouped by (Day, Week, Month)&lt;br&gt;• Most commonly detected violative clients (10, 25, 50, 100)&lt;br&gt;• Service violation report, grouped by (Day, Week, Month)</td>
</tr>
<tr>
<td>Trend Micro Total Discovery Appliance Reports</td>
<td>• Incident summary report, grouped by (Day, Week, Month)&lt;br&gt;• High risk clients (10, 25, 50, 100)&lt;br&gt;• Summary of known and unknown risks report</td>
</tr>
</tbody>
</table>
### Table A-21. Data Loss Prevention Reports and Report Types

<table>
<thead>
<tr>
<th>Data Loss Prevention Reports</th>
<th>Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top DLP Incident Sources</td>
<td>• Incidents by sender (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by host name (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by recipient (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by source IP address (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by URL (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by User (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Top template matches (10, 20, 30, 40, 50)</td>
</tr>
<tr>
<td></td>
<td>• Incident distribution by channel</td>
</tr>
<tr>
<td></td>
<td>• Incident trend, grouped by (Day, Week, Month)</td>
</tr>
<tr>
<td></td>
<td>• Incidents by channel, grouped by (Day, Week, Month)</td>
</tr>
<tr>
<td>DATA LOSS PREVENTION REPORTS</td>
<td>REPORT TYPES</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Significant Incident Increase | • Significant incident increase (%) by channel (10, 20, 30, 40, 50)  
• Significant incident increase by channel (10, 20, 30, 40, 50)  
• Significant incident increase (%) by sender (10, 20, 30, 40, 50)  
• Significant incident increase by sender (10, 20, 30, 40, 50)  
• Significant incident increase (%) by host name (10, 20, 30, 40, 50)  
• Significant incident increase by host name (10, 20, 30, 40, 50)  
• Significant incident increase (%) by user (10, 20, 30, 40, 50)  
• Significant incident increase by user (10, 20, 30, 40, 50)  
• Significant incident increase (%) by source IP address (10, 20, 30, 40, 50)  
• Significant incident increase by source IP address (10, 20, 30, 40, 50)  
• Significant incident increase (%) by template (10, 20, 30, 40, 50)  
• Significant incident increase by template (10, 20, 30, 40, 50) |

**Adding One-time Reports**

Control Manager supports generating one-time reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a one-time report is similar for all report types and involves the following:

1. Access the **Add One-time Report** screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

**Step 1: Access the Add One-time Report Screen and Select the Report Type**

**Procedure**

1. Navigate to Reports > One-time Reports.
   
   The One-time Reports screen appears.

2. Click Add.
   
   The Add One-time Report > Step 1: Contents screen appears.
3. Type a name for the report in the **Name** field, under Report Details.

4. Type a description for the report in the **Description** field, under Report Details.

5. Select the Control Manager template to generate the report:
   - **Control Manager 5 report template:**
     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the Report Templates screen.
   - **Control Manager 3 report template:**
     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.
     b. Select the report category on which to base the report.
     c. Select the Control Manager 3 template data on which to base the template.

6. Select the report generation format:
   - **Control Manager 5 report formats:**
     - Adobe PDF Format (*.pdf)
     - HTML Format (*.html)
     - XML Format (*.xml)
     - CSV Format (*.csv)
   - **Control Manager 3 report formats:**
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)

7. Click **Next**.
The Add One-Time Report > Step 2: Targets screen appears.

Step 2: Specify the Product/Products From Which the Report Data Generates:

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.

2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   • **All clients**: Reports generate from all Network VirusWall Enforcer devices
   • **IP range**: Reports generate from a specific IP address range
   • **Segment**: Reports generate from a specific network segment

3. Click **Next**.

The Add One-Time Report > Step 3: Time Period screen appears.
Step 3: Specify the Date That the Product/Products Produced the Data:

Procedure

1. Specify the data generation date:
   • From the drop down list select one of the following:
     • All dates
     • Last 24 hours
     • Today
     • Last 7 days
     • Last 14 days
     • Last 30 days
   • Specify a date range:
     • Type a date in the **From** field.
     • Specify a time in the accompanying **hh** and **mm** fields.
     • Type a date in the **To** field.
     • Specify a time in the accompanying **hh** and **mm** fields.
Introducing Trend Micro Control Manager

Note
Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**.

The **Add Onetime Report > Step 4: Message Content and Recipients** screen appears.

---

**Step 4: Specify the Recipient of the Report:**

**Procedure**

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.
5. Select the users/groups to receive the report and click the **>>** button.
6. Click Finish after selecting all users/groups to receive the report.

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a scheduled report is similar for all report types:

1. Access the Add Scheduled Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Step 1: Access the Add Scheduled Report Screen and Select the Report Type

Procedure

1. Navigate to Reports > Scheduled Reports.

The Scheduled Reports screen appears.

2. Click Add.

The Add Scheduled Report > Step 1: Contents screen appears.
3. Type a name for the report in the **Name** field.

4. Type a meaningful description for the report in the **Description** field.

5. Select the Control Manager template to generate the report:
   - Control Manager 5 report template:
     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the Report Templates screen.
   - Control Manager 3 report template:
     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.
     b. Select the report category on which to base the report.
     c. Select the Control Manager 3 template data on which to base the template.

6. Select the report generation format:
   - Control Manager 5 report formats:
     - Adobe PDF Format (*.pdf)
• HTML Format (*.html)
• XML Format (*.xml)
• CSV Format (*.csv)

• Control Manager 3 report formats:
  • Rich Text Format (*.rtf)
  • Adobe PDF Format (*.pdf)
  • ActiveX
  • Crystal Report Format (*.rpt)

7. Click Next.

The Add Scheduled Report > Step 2: Targets screen appears.
Step 2: Specify the Product/Products from Which the Report Data Generates

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.

2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment

3. Click Next.

The **Add One-Time Report > Step 3: Frequency** screen appears.
Step 3: Specify the Date that the Product/Products Produced the Data

Procedure

1. Specify how often reports generate:
   - **Daily**: Reports generate daily.
   - **Weekly**: Reports generate weekly on the specified day.
   - **Bi-weekly**: Reports generate every two weeks on the specified day.
   - **Monthly**: Reports generate monthly on the first day of the month, the 15th of the month, or the last day of the month.

2. Specify the data range:
   - **Reports include data up to the Start the schedule time specified below**: This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can make a "daily" report with almost two days worth of data depending on the Start schedule time.
   - **Reports include data up to 23:59:59 of the previous day**: This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.

3. Specify when the report schedule starts:
   - **Immediately**: The report schedule starts immediately after enabling the report.
   - **Start on**: The report schedule starts on the date and time specified in the accompanying fields.
     a. Type a date in the **mm/dd/yyyy** field.
     b. Specify a time in the accompanying **hh** and **mm** fields.
Note
Click the calendar icon next to the mm/dd/yyyy field to use a dynamic calendar to specify the date range.

4. Click Next.

The Add Scheduled Report > Step 4: Message Content and Recipients screen appears.

---

Step 4: Specify the Recipient of the Report

Procedure

1. Type a title for the email message that contains the report in the Subject field.
2. Type a description about the report in the Message field.
3. Select Email the report as an attachment to enable sending the report to a specified recipient.
4. Specify to select users or groups from the Report Recipients list.
5. Select the users/groups to receive the report and click the >> button.
6. Click **Finish** after selecting all users/groups to receive the report.
Appendix B

PolicyServer Message IDs

The following table explains PolicyServer error messages. Use it to find a Message ID, to understand the associated message meaning, the category of the message, and which agents/products the message affects.

**Table B-1. PolicyServer Message IDs**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>MESSAGE ID</th>
<th>DESCRIPTION</th>
<th>PRODUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Alerts</td>
<td>100002</td>
<td>Identifying Device</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100003</td>
<td>Security Violation</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100007</td>
<td>Critical Severity</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100019</td>
<td>Policy Change Unsuccessful</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100045</td>
<td>Unsupported configuration</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100046</td>
<td>Enterprise Pool created</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100047</td>
<td>Enterprise Pool deleted</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100048</td>
<td>Enterprise Pool modified</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100049</td>
<td>Admin User locked due to too many failed logins.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100052</td>
<td>Policy Value Integrity Check Failed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100053</td>
<td>Policy request aborted due to failed policy integrity check.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100054</td>
<td>File request aborted due to failed policy integrity check.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100055</td>
<td>Admin Authentication Succeeded</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100056</td>
<td>Admin Authentication Failed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100062</td>
<td>Admin Password Reset</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100463</td>
<td>Unable to remove user. Try again.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100464</td>
<td>Unable to unable user. Try again.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>100470</td>
<td>Unable to change Self Help password. A response to one of the personal challenge questions was incorrect.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>102000</td>
<td>Enterprise Added</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>102001</td>
<td>Enterprise Deleted</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>102002</td>
<td>Enterprise Modified</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>102003</td>
<td>The number of users has exceeded the maximum allowed by this license. Reduce the number of existing users to restore this user account.</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200000</td>
<td>Administrator updated policy</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200001</td>
<td>Administrator added policy</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200002</td>
<td>Administrator deleted policy</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>--------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200003</td>
<td>Administrator enabled application</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200004</td>
<td>Administrator disabled application</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200100</td>
<td>Administrator added user</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200101</td>
<td>Administrator deleted user</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200102</td>
<td>Administrator updated user</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200103</td>
<td>Administrator added user to group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200104</td>
<td>Administrator removed user from group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200200</td>
<td>User added</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200201</td>
<td>User deleted</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200202</td>
<td>User added to group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200203</td>
<td>User removed from group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200204</td>
<td>User updated</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200300</td>
<td>Administrator deleted device</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200301</td>
<td>Administrator added device to group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200302</td>
<td>Administrator removed device from group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200500</td>
<td>Administrator added group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200501</td>
<td>Administrator deleted group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200502</td>
<td>Administrator updated group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200503</td>
<td>Administrator copy/pasted group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200600</td>
<td>PolicyServer update applied.</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200602</td>
<td>User added to device</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200603</td>
<td>User removed from device</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200700</td>
<td>Event executed successfully</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200701</td>
<td>Failed event execution</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200800</td>
<td>Event installed successfully</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>200801</td>
<td>Failed to install event</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700012</td>
<td>Administrator Logged In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700013</td>
<td>Administrator Logged In Using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700014</td>
<td>Administrator Logged In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700017</td>
<td>Administrator Logged In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700030</td>
<td>Administrator Failed log In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700031</td>
<td>Administrator Failed log In using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700032</td>
<td>Administrator Failed log In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>700035</td>
<td>Administrator Failed log In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900100</td>
<td>Administrator logged in using one-time password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900101</td>
<td>Administrator logged in using fixed password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900102</td>
<td>Administrator logged in using Smart Card.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900103</td>
<td>Administrator logged in using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900104</td>
<td>Administrator logged in using remote authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900105</td>
<td>Administrator logged in using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900106</td>
<td>Administrator logged in using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900107</td>
<td>Administrator logged in using OCSP.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900250</td>
<td>Administrator Failed To Login Using One Time Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900251</td>
<td>Administrator Failed To Login Using Fixed Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900252</td>
<td>Administrator Failed To Login Using Smart Card</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900253</td>
<td>Administrator failed to login using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900254</td>
<td>Administrator Failed To Login Using Remote Authentication</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900255</td>
<td>Administrator failed to login using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900256</td>
<td>Administrator failed to login using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900257</td>
<td>Administrator Failed To Login Using OCSP</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>900300</td>
<td>Administrator Failed log In Using Remote Authentication</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>901000</td>
<td>Administrator Renamed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>901001</td>
<td>Administrator Changed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>901002</td>
<td>Administrator Deleted A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Administrator Alerts</td>
<td>901003</td>
<td>Administrator Created A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>100015</td>
<td>Log Message</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103000</td>
<td>Audit Log Connection Opened</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103001</td>
<td>Audit Log Connection Closed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103100</td>
<td>Audit Log Record Missing</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103101</td>
<td>Audit Log Record Integrity Missing</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103102</td>
<td>Audit Log Record Integrity Compromised</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>103103</td>
<td>Audit Log Record Integrity Validation Started</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>104003</td>
<td>Authentication method set to SmartCard.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Audit Log Alerts</td>
<td>904008</td>
<td>Unable To Send Log Alert</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700006</td>
<td>Authenticator Logged In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700007</td>
<td>Authenticator Logged In Using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700008</td>
<td>Authenticator Logged In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700009</td>
<td>Authenticator Logged In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700011</td>
<td>Authenticator Logged In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700024</td>
<td>Authenticator Failed log In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700025</td>
<td>Authenticator Failed log In Using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700026</td>
<td>Authenticator Failed log In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700027</td>
<td>Authenticator Failed log In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>700029</td>
<td>Authenticator Failed log In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900050</td>
<td>Authenticator logged in using one-time password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900051</td>
<td>Authenticator logged in using fixed password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900052</td>
<td>Authenticator logged in using Smart Card.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900053</td>
<td>Authenticator logged in using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900054</td>
<td>Authenticator logged in using remote authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900055</td>
<td>Authenticator logged in using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900056</td>
<td>Authenticator logged in using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900057</td>
<td>Authenticator logged in using OCSP.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900161</td>
<td>User Failed To Login Using Self Help</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900200</td>
<td>Authenticator Failed To Login Using One Time Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900201</td>
<td>Authenticator Failed To Login Using Fixed Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900202</td>
<td>Authenticator Failed To Login Using Smart Card</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900203</td>
<td>Authenticator failed to login using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900204</td>
<td>Authenticator Failed To Login Using Remote Authentication</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900205</td>
<td>Authenticator failed to login using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900206</td>
<td>Authenticator failed to login using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>900207</td>
<td>Authenticator Failed To Login Using OCSP</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>902000</td>
<td>Authenticator Renamed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>902001</td>
<td>Authenticator Changed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>902002</td>
<td>Authenticator Deleted A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Authenticator Alerts</td>
<td>902003</td>
<td>Authenticator Created A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Certificate Alerts</td>
<td>104008</td>
<td>Certificate expired.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100001</td>
<td>PDA to Desktop Sync Authentication was unsuccessful. There was no device ID</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for this PDA found.</td>
<td></td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100012</td>
<td>Device is not in its own Password Authentication File. PAF corrupted?</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100044</td>
<td>Lock Device Action Received</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100071</td>
<td>Device Kill Confirmed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100072</td>
<td>Device Lock Confirmed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100100</td>
<td>Install Started</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100101</td>
<td>Install Completed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>100462</td>
<td>Unable to connect to PolicyServer.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>101001</td>
<td>The network connection is not working. Unable to get policy files from PolicyServer.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>101002</td>
<td>Corrupted PAF (DAFolder.xml) file</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>105000</td>
<td>Unable to synchronize policies with client. Verify that there is a network connection and try again.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200400</td>
<td>Device added</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200401</td>
<td>Device deleted</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200402</td>
<td>Device added to group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200403</td>
<td>Device removed from group</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200404</td>
<td>Device modified</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200405</td>
<td>Device status updated</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200406</td>
<td>Device status reset</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200407</td>
<td>Device Kill Issued</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-----------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200408</td>
<td>Device Lock Issued</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>200409</td>
<td>Device Synchronized</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>904012</td>
<td>User Not Allowed To Register New Device</td>
<td>PolicyServer</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>1000052</td>
<td>Uninstall of product</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor</td>
</tr>
<tr>
<td>Device Alerts</td>
<td>1000053</td>
<td>Product Uninstall Denied By Policy</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor</td>
</tr>
<tr>
<td>Error Alerts</td>
<td>100005</td>
<td>General Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Error Alerts</td>
<td>100006</td>
<td>Application Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700000</td>
<td>User Logged In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700001</td>
<td>User Logged In Using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700002</td>
<td>User Logged In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700003</td>
<td>User Logged In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700005</td>
<td>User Logged In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700015</td>
<td>Administrator Logged In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700018</td>
<td>User Failed log In Using One Time Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700019</td>
<td>User Failed log In Using Fixed Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700020</td>
<td>User Failed log In using Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700021</td>
<td>User Failed log In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700023</td>
<td>User Could not log In Using Remote Authentication</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700033</td>
<td>Administrator Failed log In using Windows Credentials</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>700036</td>
<td>Failed Login Attempts Exceeded</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701000</td>
<td>Encrypted File Using User Key</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701001</td>
<td>Encrypted File Using Group Key</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701002</td>
<td>Encrypted File Using Static Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701003</td>
<td>Self-extracting encrypted file created using a static password.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701004</td>
<td>Encrypted File Using Cert</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701005</td>
<td>Self-extracting encrypted file created using certificate.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701006</td>
<td>Encrypted File Using CD/DVD Burning</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701007</td>
<td>Encrypted Directory Using Group Key</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701008</td>
<td>Encrypted Directory Using Static Password</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701009</td>
<td>Self-extracting encrypted directory created using a static password.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701010</td>
<td>Encrypted Directory Using Cert</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701011</td>
<td>Self-extracting encrypted directory created using certificate.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701012</td>
<td>Encrypted Directory Using CD/DVD Burning</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701015</td>
<td>Removable Media was fully encrypted</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701016</td>
<td>Removable Media Blocked</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701017</td>
<td>Removable Media Created and Covered Folders</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701018</td>
<td>File encrypted and moved to removable media.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>701019</td>
<td>File deleted from removable media.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>703000</td>
<td>File Armor Encrypted Folder Was Created</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>703001</td>
<td>Folder Was Created and Covered</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>703002</td>
<td>File Armor Encrypted Folder Was Deleted</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>703004</td>
<td>Removable Media Folder was Created and Covered</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703005</td>
<td>Removable Media Device Was Fully Encrypted</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703006</td>
<td>File In Folder Was Created</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703007</td>
<td>File in Folder Was Deleted</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703008</td>
<td>File in Folder Was Changed</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703009</td>
<td>File in Folder Was Accessed</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703010</td>
<td>File in Folder Was Last Written</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703011</td>
<td>File Size Changed in Folder</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703015</td>
<td>Folder Encryption Started</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703016</td>
<td>Folder Decryption Started</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703017</td>
<td>Folder Encryption Complete</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703018</td>
<td>Folder Decryption Complete</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>703019</td>
<td>Folder Decryption In progress</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>File Encryption Activity</td>
<td>703020</td>
<td>Folder Decryption In progress</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Alerts</td>
<td>704000</td>
<td>File Encryption Service Started</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>File Encryption Activity Alerts</td>
<td>704001</td>
<td>File Encryption Service Shutdown</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>300700</td>
<td>Device log maximum size limit reached, event log truncated.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400001</td>
<td>User has successfully logged in.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400002</td>
<td>User login failed.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400003</td>
<td>Device decryption started.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400004</td>
<td>Device Encryption Started.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400005</td>
<td>Mounted encrypted partition.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400006</td>
<td>Restored native OS MBR.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400007</td>
<td>Restored Application MBR.</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400008</td>
<td>Device encryption complete</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400009</td>
<td>Device Decryption Completed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400010</td>
<td>Device Encryption In Progress</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400011</td>
<td>System MBR Corrupt</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>400012</td>
<td>System Pre-boot Kernel Deleted</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401000</td>
<td>Recovery Console accessed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401009</td>
<td>Recovery Console error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401010</td>
<td>Decryption in place started</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401011</td>
<td>Decryption in place stopped</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401012</td>
<td>Decryption in place complete</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401013</td>
<td>Decryption of removable device started</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401014</td>
<td>Decryption to removable device stopped</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401015</td>
<td>Decryption to removable device complete</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401018</td>
<td>Decryption in place error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401019</td>
<td>Decryption to removable device error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401020</td>
<td>Encrypted files accessed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401021</td>
<td>Encrypted files modified</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401022</td>
<td>Encrypted files copied to removable device</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401029</td>
<td>Encrypted files access error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401030</td>
<td>Network administration accessed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401031</td>
<td>PolicyServer address changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401032</td>
<td>PolicyServer port number changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401033</td>
<td>Switched to IPv6</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401034</td>
<td>Switched to IPv4</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401035</td>
<td>Switched to dynamic IP configuration</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401036</td>
<td>Switched to static IP configuration</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401037</td>
<td>DHCP port number changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401038</td>
<td>IP address changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401039</td>
<td>NetMask changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>401040</td>
<td>Broadcast address changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401041</td>
<td>Gateway changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401042</td>
<td>Domain name changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401043</td>
<td>Domain name servers changed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401049</td>
<td>Network administration error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401050</td>
<td>User administration accessed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401051</td>
<td>User added</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401052</td>
<td>User removed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401053</td>
<td>User modified</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401069</td>
<td>User administration error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401070</td>
<td>Locally stored logs accessed</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401079</td>
<td>Locally stored logs access error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401080</td>
<td>Original MBR restored</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401089</td>
<td>Original MBR restoration error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401090</td>
<td>Default theme restored</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption Activity</td>
<td>401099</td>
<td>Default theme restoration error</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>402000</td>
<td>Application Startup</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>402001</td>
<td>Application Shutdown</td>
<td>Full Disk Encryption or MobileSentinel</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>600001</td>
<td>Update was successful in the Pre-boot.</td>
<td>Full Disk Encryption</td>
</tr>
<tr>
<td>Full Disk Encryption Activity Alerts</td>
<td>600002</td>
<td>Pre-boot Update failed</td>
<td>Full Disk Encryption</td>
</tr>
<tr>
<td>Installation Alerts</td>
<td>100004</td>
<td>Install Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Installation Alerts</td>
<td>100020</td>
<td>Successful Installation</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Installation Alerts</td>
<td>700037</td>
<td>Installation of File Encryption was successful</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Installation Alerts</td>
<td>700038</td>
<td>Installation of File Encryption was unsuccessful: Enterprise name is not valid.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Installation Alerts</td>
<td>700039</td>
<td>Installation of File Encryption was unsuccessful: Username or password is incorrect.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>100034</td>
<td>Invalid Registry Setting Detected</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500000</td>
<td>VirusDefense</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500001</td>
<td>Object Cleaned</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500002</td>
<td>Object Disinfected</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500003</td>
<td>Object Quarantined</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500004</td>
<td>Object Deleted</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500005</td>
<td>Virus Detected</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500006</td>
<td>Full Scan Started</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500007</td>
<td>Full Scan Completed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500008</td>
<td>Object Suspicious</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500009</td>
<td>Object Scan Completed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500010</td>
<td>Removable Media Scan Requested</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>500011</td>
<td>Removable Media Scan Completed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500012</td>
<td>Folder Scan Requested</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500013</td>
<td>Folder Scan Completed</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500014</td>
<td>Access Denied To Object</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500015</td>
<td>Object Corrupt</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500016</td>
<td>Object Clean</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500017</td>
<td>Full Scan Cancelled</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500018</td>
<td>Object Scan Cancelled</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500019</td>
<td>Removable Media Scan Cancelled</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500020</td>
<td>Folder Scan Cancelled</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500021</td>
<td>Update Started</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500022</td>
<td>The update was unsuccessful. Try again.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500023</td>
<td>Update Cancelled</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500024</td>
<td>Update Successful.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500025</td>
<td>VirusDefense Up To Date</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500026</td>
<td>PalmVirusDefense</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500027</td>
<td>Object Scan Requested</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>500028</td>
<td>PPCVirusDefense</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900000</td>
<td>User logged in using one-time password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900001</td>
<td>User logged in using fixed password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900002</td>
<td>User logged in using Smart Card.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900003</td>
<td>User logged in using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900004</td>
<td>User logged in using remote authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900005</td>
<td>User logged in using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900006</td>
<td>User logged in using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900007</td>
<td>User logged in using OCSP</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900008</td>
<td>User logged in using Self Help.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900009</td>
<td>User logged in using RSA</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900150</td>
<td>User Failed To Login Using One Time Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900151</td>
<td>User Failed To Login Using Fixed Password</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900152</td>
<td>User Failed To Login Using Smart Card</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900153</td>
<td>User failed to login using domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900154</td>
<td>User Failed To Login Using Remote Authentication</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900155</td>
<td>User failed to login using ColorCode authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900156</td>
<td>User failed to login using PIN.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900157</td>
<td>User Failed To Login Using OCSP</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900158</td>
<td>User locked out after too many failed login attempts.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900301</td>
<td>Failed Login Attempts Exceeded</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>900350</td>
<td>Key Wiped</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>903000</td>
<td>User Renamed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>KeyArmor Activity</td>
<td>903001</td>
<td>User Changed A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Alerts</td>
<td>903002</td>
<td>User Deleted A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>903003</td>
<td>User Created A File</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>903100</td>
<td>Primary action enforced due to no PolicyServer connection.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>903101</td>
<td>Secondary action enforced due to no PolicyServer connection.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>903102</td>
<td>Policy updates applied</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904000</td>
<td>Repaired infected file</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904001</td>
<td>Unable to repair infected file.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904002</td>
<td>Skipping infected file, repair unsupported</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904003</td>
<td>Deleted infected file</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904004</td>
<td>Unable to delete infected file.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904005</td>
<td>Killing device due to infected file</td>
<td>KeyArmor</td>
</tr>
<tr>
<td></td>
<td>904006</td>
<td>Error killing device due to infected file</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>904007</td>
<td>Invoking infected file fall-back action</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>904010</td>
<td>AntiVirus files updated</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>KeyArmor Activity Alerts</td>
<td>904011</td>
<td>Unable to update antivirus files.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100013</td>
<td>Failed Login Attempt</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100014</td>
<td>Successful Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100016</td>
<td>Unable to log in. Use Remote Authentication to provide the PolicyServer Administrator with a challenge code.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100021</td>
<td>Unsuccessful ColorCode Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100022</td>
<td>Unsuccessful Fixed Password Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100023</td>
<td>Unsuccessful PIN Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100024</td>
<td>Unsuccessful X99 Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100028</td>
<td>Successful ColorCode Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100031</td>
<td>Successful X9.9 Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100032</td>
<td>Successful Remote Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100035</td>
<td>Successful WebToken Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100036</td>
<td>Unsuccessful WebToken Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100050</td>
<td>Fixed Password login blocked due to lockout.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100051</td>
<td>User Login Successfully Unlocked</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100057</td>
<td>LDAP User Authentication Succeeded</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100058</td>
<td>LDAP User Authentication Failed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100059</td>
<td>LDAP User Password Change Succeeded</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100060</td>
<td>LDAP User Password Change Failed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100061</td>
<td>Access request aborted due to failed policy integrity check.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100070</td>
<td>Successful Logout</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100433</td>
<td>The ColorCode passwords do not match.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100434</td>
<td>Unable to change ColorCode. The new ColorCode must be different than the current one.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100435</td>
<td>Unable to change ColorCode. The new ColorCode must meet the minimum length requirements defined by PolicyServer.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100436</td>
<td>Unable to change ColorCode. The new ColorCode must be different than any previous ColorCode used.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100437</td>
<td>ColorCode Change Failure - Internal Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100459</td>
<td>X9.9 Password Change Failure - Can Not Connect to PolicyServer Host</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100460</td>
<td>X9.9 Password Change Failure - Empty Serial Number</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>100461</td>
<td>X9.9 Password Change Failure - Internal Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>101004</td>
<td>Unable to reset locked device.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>104000</td>
<td>Smart Card login successful.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Login / Logout Alerts</td>
<td>104001</td>
<td>Smart Card login unsuccessful. Check that the card is seated properly and that the Smart Card PIN is valid.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Mobile Device Alert</td>
<td>100037</td>
<td>Palm Policy Database is missing</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Category</td>
<td>Message ID</td>
<td>Description</td>
<td>Products</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile Device Alert</td>
<td>100038</td>
<td>Palm Encryption Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Mobile Device Alert</td>
<td>100039</td>
<td>PPC Device Encryption Changed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Mobile Device Alert</td>
<td>100040</td>
<td>PPC Encryption Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>MobileFirewall Activity Alerts</td>
<td>300000</td>
<td>MobileFirewall</td>
<td>MobileFirewall</td>
</tr>
<tr>
<td>MobileFirewall Activity Alerts</td>
<td>300001</td>
<td>DenialOfServiceAttack</td>
<td>MobileFirewall</td>
</tr>
<tr>
<td>OCSP Alerts</td>
<td>104005</td>
<td>OCSP certificate status good.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>OCSP Alerts</td>
<td>104006</td>
<td>OCSP certificate status revoked.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>OCSP Alerts</td>
<td>104007</td>
<td>OCSP certificate status unknown.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OTA Alerts</td>
<td>100041</td>
<td>OTA Object Missing or Corrupt.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>OTA Alerts</td>
<td>100042</td>
<td>OTA Sync Successful</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>OTA Alerts</td>
<td>100043</td>
<td>OTA Device Killed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100017</td>
<td>Change Password Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100018</td>
<td>Password Attempts Exceeded</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100025</td>
<td>Password Reset to ColorCode</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100026</td>
<td>Password Reset to Fixed</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100027</td>
<td>Password Reset to PIN</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100029</td>
<td>Successful Fixed Password Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100030</td>
<td>Successful PIN Password Login</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100033</td>
<td>Unable to Reset Password</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100432</td>
<td>Unable to change password. The new password must be different than the current password.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100439</td>
<td>Unable to change password. The passwords do not match.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100441</td>
<td>Unable to change password. The password field cannot be empty.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100442</td>
<td>Unable to change password. The password does not meet the minimum length requirements defined by PolicyServer.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100443</td>
<td>Unable to change password. Numbers are not permitted.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100444</td>
<td>Unable to change password. Letters are not permitted.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100445</td>
<td>Unable to change password. Special characters are not permitted.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100446</td>
<td>Unable to change password. The password cannot contain the user name.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100447</td>
<td>Unable to change password. The password does not contain enough special characters.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100448</td>
<td>Unable to change password. The password does not contain enough numbers.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100449</td>
<td>Unable to change password. The password does not contain enough characters.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100450</td>
<td>Unable to change password. The password contains too many consecutive characters.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100451</td>
<td>Unable to change password. The new password must be different than any previous password used.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>100452</td>
<td>Password Change Failure - Internal Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>101003</td>
<td>Successfully changed Fixed Password.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>700100</td>
<td>Password reset to Fixed Password.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>700101</td>
<td>Password reset to Smart Card</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>700102</td>
<td>Password reset to Domain Authentication.</td>
<td>File Encryption SP6 or Earlier</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>900159</td>
<td>Unable to change password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>900160</td>
<td>Password changed successfully.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>900302</td>
<td>Password reset to fixed password.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>900303</td>
<td>Password reset To Smart Card</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>Password Alerts</td>
<td>900304</td>
<td>Password reset to domain authentication.</td>
<td>KeyArmor</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100438</td>
<td>Unable to change PIN. The PINs do not match.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100440</td>
<td>Unable to change PIN. One of the fields are empty.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100453</td>
<td>Unable to change PIN. The PINs do not match.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100454</td>
<td>able to change PIN. The new PIN cannot be the same as the old PIN.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100455</td>
<td>Unable to change PIN. The new PIN does not meet the minimum length requirements defined by PolicyServer.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100456</td>
<td>Unable to change PIN. The PIN cannot contain the user name.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100457</td>
<td>Unable to change PIN. The new PIN must be different than any previous PIN used.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>PIN Change Alerts</td>
<td>100458</td>
<td>PIN Change Failure - Internal Error</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Smart Card Alerts</td>
<td>104002</td>
<td>Registered SmartCard.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>MESSAGE ID</td>
<td>DESCRIPTION</td>
<td>PRODUCTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart Card Alerts</td>
<td>104004</td>
<td>Unable to register Smart Card. Check that the card is seated properly and that the Smart Card PIN is valid.</td>
<td>Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800000</td>
<td>OTA Install started</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800001</td>
<td>OTA Install completed</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800100</td>
<td>OTA SMS message sent</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800200</td>
<td>OTA Directory Listing Received</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800300</td>
<td>OTA Device Attributes Received</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800400</td>
<td>OTA Device Backup</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
<tr>
<td>Windows Mobile Alerts</td>
<td>800500</td>
<td>OTA Device Restore</td>
<td>Full Disk Encryption for Windows Mobile</td>
</tr>
</tbody>
</table>
### Endpoint Encryption Services

The following table describes all Endpoint Encryption services. Use it to understand which services control which Endpoint Encryption agent or feature and to troubleshoot a problem.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service 1</td>
<td>Description 1</td>
</tr>
<tr>
<td>Service 2</td>
<td>Description 2</td>
</tr>
<tr>
<td>Service 3</td>
<td>Description 3</td>
</tr>
<tr>
<td>Service 4</td>
<td>Description 4</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Platform</th>
<th>Service or Daemon Name</th>
<th>Display Name</th>
<th>Description</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMEEService</td>
<td>Endpoint Encryption Service</td>
<td>Endpoint Encryption Service</td>
<td>Manages Endpoint Encryption agent 5.0 (and above) communication in an encrypted channel (RESTful).</td>
<td>TMEEService.exe</td>
</tr>
<tr>
<td>IIS/MAWebService2</td>
<td>Legacy Web Service</td>
<td>Legacy Web Service</td>
<td>Manages Endpoint Encryption agent 3.1.3 (and older) communication in an encrypted channel (SOAP).</td>
<td>N/A</td>
</tr>
<tr>
<td>TMEEForward</td>
<td>TMEEForward</td>
<td>TMEEForward</td>
<td>Forwards traffic from Endpoint Encryption 5.0 agents to PolicyServer.</td>
<td>TMEEForward.exe</td>
</tr>
<tr>
<td>TMEEProxyWindowsService</td>
<td>PolicyServer LDAPProxy Windows Service</td>
<td>Provides secure communications from Trend Micro PolicyServer to remote LDAP servers</td>
<td>LDAPProxyWindowsService.exe</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Service or Daemon Name</td>
<td>Display Name</td>
<td>Description</td>
<td>File Name</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>DrAService</td>
<td>Trend Micro Full Disk Encryption</td>
<td>Provides Trend Micro endpoint security and full disk encryption.</td>
<td>DrAService.exe</td>
</tr>
<tr>
<td>Encryption Management for Microsoft BitLocker</td>
<td>FDE_MB</td>
<td>Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker</td>
<td>Provides data security for endpoints using Microsoft BitLocker.</td>
<td>FDEforBitLocker.exe</td>
</tr>
<tr>
<td>File Encryption</td>
<td>FileEncryption Service</td>
<td>Trend Micro File Encryption</td>
<td>Provides Trend Micro endpoint security and data protection for files, folders, and removable media devices.</td>
<td>FEService.exe</td>
</tr>
</tbody>
</table>
Policy Mapping Between Management Consoles

Administrators may manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

The following tables explain how policies are mapped between PolicyServer MMC and Control Manager. For environments using Control Manager to manage PolicyServer, use PolicyServer MMC to control any policy not listed in the table.

**TABLE D-1. Full Disk Encryption Policy Mapping**

<table>
<thead>
<tr>
<th>CONTROL MANAGER LABEL</th>
<th>POLICYSERVER MMC PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Encrypt endpoint</td>
<td>Full Disk Encryption &gt; Encryption &gt; Encrypt Device</td>
</tr>
<tr>
<td>Client Settings</td>
<td></td>
</tr>
<tr>
<td>Bypass Full Disk Encryption preboot</td>
<td>Full Disk Encryption &gt; Login &gt; Preboot Bypass</td>
</tr>
<tr>
<td>Users are allowed to access system recovery tools on the device</td>
<td>Full Disk Encryption &gt; Agent &gt; Allow User Recovery</td>
</tr>
</tbody>
</table>
### TABLE D-2. File Encryption Policy Mapping

<table>
<thead>
<tr>
<th>CONTROL MANAGER LABEL</th>
<th>POLICY SERVER MMC PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification</strong></td>
<td></td>
</tr>
<tr>
<td>If the endpoint is found, display the following message</td>
<td>Full Disk Encryption &gt; Login &gt; If Found</td>
</tr>
<tr>
<td>Display Technical Support contact information</td>
<td>Full Disk Encryption &gt; Login &gt; Support Info</td>
</tr>
<tr>
<td>Show legal notice</td>
<td></td>
</tr>
<tr>
<td>• Show legal notice &gt; Installation</td>
<td>Full Disk Encryption &gt; Login &gt; Legal Notice &gt; Legal Notice Display Time</td>
</tr>
<tr>
<td>• Show legal notice &gt; Startup</td>
<td>Full Disk Encryption &gt; Login &gt; Legal Notice &gt; Legal Notice Text</td>
</tr>
</tbody>
</table>

| Folders to Encrypt    |                        |
| Folders to Encrypt text box | File Encryption > Encryption > Specify Folders to Encrypt |

| Encryption Key Used   |                        |
| Encryption Key Used    | File Encryption > Encryption > Encryption Key Used |

<p>| Storage Devices       |                        |
| Disable optical drives | File Encryption &gt; Encryption &gt; Disable Optical Drive |
| Disable USB drives     | File Encryption &gt; Encryption &gt; Removable Media &gt; Disable USB Drive |</p>
<table>
<thead>
<tr>
<th><strong>CONTROL MANAGER LABEL</strong></th>
<th><strong>POLICY SERVER MMC PATH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt all files and folders on USB drives</td>
<td>File Encryption &gt; Encryption &gt; Removable Media &gt; Fully Encrypt Device</td>
</tr>
<tr>
<td>Specify the file path to encrypt on USB devices</td>
<td>File Encryption &gt; Encryption &gt; Removable Media &gt; Folders to Encrypt On Removable Media</td>
</tr>
<tr>
<td>Notifications</td>
<td></td>
</tr>
<tr>
<td>Show legal notice</td>
<td>File Encryption &gt; Login &gt; Legal Notice</td>
</tr>
<tr>
<td>• Show legal notice &gt; Installation</td>
<td>File Encryption &gt; Login &gt; Legal Notice &gt; Legal Notice Display Time</td>
</tr>
<tr>
<td>• Show legal notice &gt; Startup</td>
<td></td>
</tr>
<tr>
<td>Show legal notice text box</td>
<td>File Encryption &gt; Login &gt; Legal Notice &gt; Legal Notice Text</td>
</tr>
</tbody>
</table>

**Table D-3. Common Policy Mapping**

<table>
<thead>
<tr>
<th><strong>CONTROL MANAGER LABEL</strong></th>
<th><strong>POLICY SERVER MMC PATH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow User to Uninstall</td>
<td></td>
</tr>
<tr>
<td>Allow non-administrator accounts to uninstall agent software</td>
<td>• Full Disk Encryption &gt; Agent &gt; Allow User to Uninstall</td>
</tr>
<tr>
<td></td>
<td>• File Encryption &gt; Agent &gt; Allow User to Uninstall</td>
</tr>
<tr>
<td>Lockout and Lock Device Actions</td>
<td></td>
</tr>
<tr>
<td>Lock account after <code>&lt;number&gt;</code> days</td>
<td>Full Disk Encryption &gt; Login &gt; Account Lockout Period</td>
</tr>
<tr>
<td>Account lockout action</td>
<td>Full Disk Encryption &gt; Login &gt; Account Lockout Action</td>
</tr>
<tr>
<td>Failed logon attempts allowed</td>
<td>Full Disk Encryption &gt; Login &gt; Failed Login Attempts Allowed</td>
</tr>
<tr>
<td><strong>CONTROL MANAGER LABEL</strong></td>
<td><strong>POLICY SERVER MMC PATH</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Full Disk Encryption:</td>
<td>Full Disk Encryption &gt; Login &gt; Device Locked Action</td>
</tr>
<tr>
<td>Device locked action</td>
<td></td>
</tr>
<tr>
<td>Full Disk Encryption:</td>
<td>Full Disk Encryption &gt; Login &gt; Lock Device Time Delay</td>
</tr>
<tr>
<td>Number of minutes to lock device</td>
<td></td>
</tr>
<tr>
<td>File Encryption:</td>
<td>File Encryption &gt; Login &gt; Device Locked Action</td>
</tr>
<tr>
<td>Device locked action</td>
<td></td>
</tr>
<tr>
<td>File Encryption:</td>
<td>File Encryption &gt; Login &gt; Lock Device Time Delay</td>
</tr>
<tr>
<td>Number of minutes to lock device</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Change Password Every</td>
</tr>
<tr>
<td>User must change password after &lt;number&gt; days</td>
<td></td>
</tr>
<tr>
<td>User cannot reuse the previous &lt;number&gt; passwords</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Password History Retention</td>
</tr>
<tr>
<td>Number of consecutive characters allowed in a password</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Consecutive Characters Allowed</td>
</tr>
<tr>
<td>Minimum length allowed for passwords</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Minimum Length</td>
</tr>
<tr>
<td>Password Character Requirements</td>
<td></td>
</tr>
<tr>
<td>Letters</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Require How Many Characters</td>
</tr>
<tr>
<td>Lowercase characters</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Require How Many Lower Case Characters</td>
</tr>
<tr>
<td>Control Manager Label</td>
<td>Policy Server MMC Path</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Uppercase characters</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Require How Many Upper Case Characters</td>
</tr>
<tr>
<td>Numbers</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Require How Many Numbers</td>
</tr>
<tr>
<td>Symbols</td>
<td>Common &gt; Authentication &gt; Local Login &gt; User Password &gt; Require How Many Special Characters</td>
</tr>
</tbody>
</table>
Appendix E

OfficeScan Integration

The following content explains how to use the Endpoint Encryption Deployment Tool OfficeScan plug-in to deploy Endpoint Encryption across an enterprise with endpoints managed by OfficeScan.

For information about PolicyServer prerequisites, OfficeScan system requirements, or managing the Endpoint Encryption Deployment Tool plug-in, see the Endpoint Encryption Installation and Migration Guide.

Topics include:

• About Trend Micro OfficeScan Integration on page E-2
• About Plug-in Manager on page E-3
• Using Plug-in Programs on page E-5
• The OfficeScan Agent Tree on page E-5
• Endpoint Encryption Agent Deployment on page E-9
About Trend Micro OfficeScan Integration

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents. The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

**Note**

For information about OfficeScan, see the supporting documentation at:


Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to deploy Endpoint Encryption agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment. After the Endpoint Encryption Deployment Tool plug-in deploys the Endpoint Encryption agent software, the Endpoint Encryption agent synchronizes to PolicyServer using the settings specified in the plug-in. OfficeScan does not manage Endpoint Encryption policies. The OfficeScan agent and the Endpoint Encryption agent are independent on the same endpoint.
The following illustration explains how to deploy Endpoint Encryption for the first time on OfficeScan managed endpoints. In OfficeScan deployments, administrators can use either Control Manager or PolicyServer MMC to manage PolicyServer.

![OfficeScan integration deployment diagram](image)

**Figure E-1. OfficeScan integration deployment**

**About Plug-in Manager**

OfficeScan includes a framework called Plug-in Manager that integrates new solutions into the existing OfficeScan environment. To help ease the management of these solutions, Plug-in Manager provides at-a-glance data for the solutions in the form of widgets.
None of the plug-in solutions currently support IPv6. The server can download these solutions but is not able to deploy the solutions to pure IPv6 Endpoint Encryption agents or pure IPv6 hosts.

Plug-in Manager delivers two types of solutions:

- **Native Product Features**

  Some native OfficeScan features are licensed separately and activated through Plug-in Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection**.

- **Plug-in programs**

  Plug-in programs are not part of the OfficeScan program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the OfficeScan web console. Examples of plug-in programs are **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)**, and **Trend Micro Mobile Security**.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets. Refer to specific plug-in program documentation for details on configuring and managing the program.

### Installing OfficeScan

For information about installing and configuring OfficeScan, see the documentation available at:


For information about installing and configuring the OfficeScan Endpoint Encryption Deployment Tool before deploying Endpoint Encryption agents, see the *Endpoint Encryption Installation and Migration Guide* for installation and configuration options.
Using Plug-in Programs

This section describes how to install and manage the OfficeScan Endpoint Encryption Deployment Tool plug-in program.

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program’s management console, which is accessible from the OfficeScan web console. Tasks include activating the program and possibly deploying the plug-in program agent to endpoints. Consult the documentation for the specific plug-in program for details on configuring and managing the program.

Managing Endpoint Encryption Deployment Tool

Procedure

1. Open the OfficeScan web console and click Plug-in Manager in the main menu.
2. On the Plug-in Manager screen, go to the plug-in program section and click Manage Program.

The OfficeScan Agent Tree

The OfficeScan agent tree displays all the agents grouped into domains that the server currently manages. Agents are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

Agent Tree Specific Tasks

The agent tree displays when you access certain screens on the web console. Above the agent tree are menu items specific to the screen you have accessed. These menu items allow you to perform specific tasks, such as configuring agent settings or initiating agent
tasks. To perform any of the tasks, first select the task target and then select a menu item.

The agent tree provides access to the following functions:

- **Search for endpoints**: Locate specific endpoints by typing search criteria in the text box.

- **Synchronize with OfficeScan**: Synchronize the plug-in program’s agent tree with the OfficeScan server’s agent tree. For details, see *Synchronizing the Agent Tree on page E-6*.

- **Deploy Server Settings**: Displays the **Deploy Server Settings** screen. For details, see *Deploying Server Settings on page E-9*.

Administrators can also manually search the agent tree to locate endpoints or domains. Specific computer information displays in the table on the right.

### Synchronizing the Agent Tree

Before the plug-in program can deploy settings to agents, administrators need to synchronize the agent tree with the OfficeScan server.

**Procedure**

1. Open the plug-in console.

2. On the **Client Management** screen, click **Synchronize with OfficeScan**.

   A confirmation message screen appears.

3. Allow a few moments for the synchronization to complete.

4. Click **Close** to return to the **Client Management** screen.

### Endpoint Encryption Agent Installation Error Codes

The following table describes the error codes for Endpoint Encryption agent installation errors. Use it to understand the problem and resolution for a specific installation error.
Note

Make sure that the endpoint meets the minimum system requirements before deploying Endpoint Encryption agents. Microsoft .Net Framework 2.0 SP1 or above is required. For information about system requirements, see the *Endpoint Encryption Installation and Migration Guide*.

**Table E-1. Installation Error Codes**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Error Code</th>
<th>Problem and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Encryption</td>
<td>1603</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>-3</td>
<td>The user name or password is invalid. Verify the credentials and try to log on to PolicyServer again.</td>
</tr>
<tr>
<td></td>
<td>-6</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td></td>
<td>-13</td>
<td>The endpoint does not meet the minimum system requirements. Upgrade the RAM or disk space and try to install the agent again.</td>
</tr>
<tr>
<td>Agent</td>
<td>Error Code</td>
<td>Problem and Resolution</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Management for Microsoft BitLocker</td>
<td>1603</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td>-13</td>
<td></td>
<td>Unable to install the Endpoint Encryption agent. Microsoft BitLocker requires Trusted Platform Module (TPM). The endpoint either does not support TPM, TPM is not enabled in BIOS, or TPM is locked by another logged on user. Enable TPM in BIOS or contact the system administrator for assistance.</td>
</tr>
</tbody>
</table>
| -14                                        |            | Unable to install the Endpoint Encryption agent. The operating system is not supported. Install one of the following supported operating systems and then try again:  
  • Windows 7 32-bit or 64-bit, Ultimate or Enterprise edition  
  • Windows 8 32-bit or 64-bit, Professional or Enterprise edition |
| -15                                        |            | Full Disk Encryption is already installed.                                               |
| -16                                        |            | Unable to install the Endpoint Encryption agent. The endpoint is already encrypted.       |
Deploying Server Settings

Configure and deploy the PolicyServer settings to ensure communication between the agents and PolicyServer.

Procedure

1. Open the plug-in program console.
2. Click the PolicyServer Settings tab.
3. Specify the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Specify the PolicyServer IP address or host name.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port number assigned to the PolicyServer instance.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Specify the PolicyServer Enterprise. Only one Enterprise is supported.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the Enterprise Administrator user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the Enterprise Administrator password.</td>
</tr>
</tbody>
</table>

4. Click Save.

A confirmation message appears. Allow some time to establish a server connection.

Endpoint Encryption Agent Deployment

This section describes how to use the Endpoint Encryption Deployment Tool Plug-in to initiate agent installation and uninstallation commands.
The following illustration shows the Endpoint Encryption Deployment Tool **Client Management** screen.

![Endpoint Encryption Deployment Tool](image)

**FIGURE E-2. Endpoint Encryption Deployment Tool**

### Deploying the Agent with OfficeScan

Before deploying agents, make sure that the endpoints meet the minimum system requirements. For more information, see the *Endpoint Encryption Installation and Migration Guide*.

**Procedure**

1. Select the endpoint from the client tree.

   **Note**

   To select multiple endpoints, hold CTRL and select applicable endpoints.

2. Click **Install**, then select one of the following options:
<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption</td>
<td>Select the appropriate Full Disk Encryption agents.</td>
</tr>
<tr>
<td></td>
<td>• Select the Full Disk Encryption agent to deploy all features, including</td>
</tr>
<tr>
<td></td>
<td>preboot authentication, all policies, notifications, and device actions.</td>
</tr>
<tr>
<td></td>
<td>• Select the Encryption Management for Microsoft BitLocker agent to enable</td>
</tr>
<tr>
<td></td>
<td>Microsoft BitLocker full disk encryption, deploying only limited policies</td>
</tr>
<tr>
<td></td>
<td>and device actions.</td>
</tr>
</tbody>
</table>

**Note**

It is not possible to deploy the Encryption Management for Apple FileVault agent using the Endpoint Encryption Deployment Tool plug-in.

| File Encryption | Deploy the File Encryption agent, which includes all features and policies. |

3. Click **Deploy**.

4. At the message, click **OK** to confirm the deployment.

The agent deployment command is initiated. If successful, any selected endpoint is prompted to restart.

### Confirming Agent Deployment

This task explains how to confirm that the Endpoint Encryption agent install initiates correctly on the endpoint.

**Procedure**

1. Complete *Deploying the Agent with OfficeScan on page E-10*.

2. Log on to the selected Endpoint Encryption device.

3. Do one of the following:
   - To view the deployment status, open the log files at:
Client endpoint
C:\TMEE_Deploy_Client.log

Server endpoint
C:\TMEE_Deploy_Server_Inst.log

- Run Task Manager and search one of the services at Endpoint Encryption Agent Services on page E-12.

4. When the Endpoint Encryption agent deployment completes, reboot the endpoint to complete the installation.

Endpoint Encryption Agent Services

The following table explains the services running when the Endpoint Encryption agent initiates on the endpoint. Use it to verify that the agent has been successfully installed and is correctly functioning.

---

**Note**

For more information about Endpoint Encryption services, see Endpoint Encryption Services on page C-1.

---

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEService.exe</td>
<td>The File Encryption agent is running.</td>
</tr>
<tr>
<td>TMFDE.exe</td>
<td>The Full Disk Encryption agent is running.</td>
</tr>
<tr>
<td>TMFDEForBitLocker.exe</td>
<td>The Encryption Management for Microsoft BitLocker agent is running.</td>
</tr>
</tbody>
</table>

Endpoint Encryption Agent Deployment Statuses

The following table explains the OfficeScan statuses that appear in the Endpoint Encryption Deployment Tool plug-in console after initiating a deployment command. Use it to understand if there was a problem during the agent installation or uninstallation.
## Table E-2. Agent Installation Statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In progress</td>
<td>In progress: agent deployment</td>
<td>OfficeScan is attempting to communicate with the managed endpoint, install the Endpoint Encryption agent, then establish a connection with PolicyServer.</td>
</tr>
<tr>
<td>Successful</td>
<td>Successful agent deployment</td>
<td>The Endpoint Encryption agent installed successfully, and has established communication with both OfficeScan and PolicyServer.</td>
</tr>
<tr>
<td>Unsuccessful</td>
<td>Unsuccessful agent deployment</td>
<td>The Endpoint Encryption agent deployment could not finish. Review the logs to find out why the managed endpoint could not update with the selected Endpoint Encryption agent.</td>
</tr>
<tr>
<td>Restart required</td>
<td>Successful agent deployment. Shutdown/Restart required.</td>
<td>For the Full Disk Encryption agent, a restart is required to complete the installation. The status is not updated until after the user has logged on the PolicyServer preboot.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timed out: agent deployment</td>
<td>The timeout period is 30 minutes. After a timeout, initiate a new deployment command.</td>
</tr>
</tbody>
</table>

## Table E-3. Agent Uninstallation Statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In progress</td>
<td>Request in progress: agent deployment</td>
<td>OfficeScan is attempting to communicate with the managed endpoint and uninstall the agent software. The managed endpoint must reply to the deployment command before the uninstallation can start.</td>
</tr>
</tbody>
</table>
The following table describes the error codes for Endpoint Encryption agent installation errors. Use it to understand the problem and resolution for a specific installation error.

<table>
<thead>
<tr>
<th>Status</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful</td>
<td>Successful agent uninstallation</td>
<td>The Endpoint Encryption agent uninstalled successfully and has established communication with OfficeScan and PolicyServer. After uninstallation, the Endpoint Encryption device is removed from PolicyServer.</td>
</tr>
<tr>
<td>Unsuccessful</td>
<td>Unsuccessful agent uninstallation</td>
<td>The Endpoint Encryption agent uninstallation request could not establish a connection. Review the logs to find out why the managed endpoint could not uninstall the Endpoint Encryption.</td>
</tr>
<tr>
<td>Restart required</td>
<td>Successful agent uninstallation. Shutdown/ Restart required.</td>
<td>For some Endpoint Encryption agents, a restart is required to complete the uninstallation.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Request timeout: agent uninstallation</td>
<td>The timeout period is 30 minutes. After a timeout, initiate a new uninstallation request.</td>
</tr>
</tbody>
</table>

### Endpoint Encryption Agent Installation Error Codes

The following table describes the error codes for Endpoint Encryption agent installation errors. Use it to understand the problem and resolution for a specific installation error.

<table>
<thead>
<tr>
<th>Status</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful</td>
<td>Successful agent uninstallation</td>
<td>The Endpoint Encryption agent uninstalled successfully and has established communication with OfficeScan and PolicyServer. After uninstallation, the Endpoint Encryption device is removed from PolicyServer.</td>
</tr>
<tr>
<td>Unsuccessful</td>
<td>Unsuccessful agent uninstallation</td>
<td>The Endpoint Encryption agent uninstallation request could not establish a connection. Review the logs to find out why the managed endpoint could not uninstall the Endpoint Encryption.</td>
</tr>
<tr>
<td>Restart required</td>
<td>Successful agent uninstallation. Shutdown/ Restart required.</td>
<td>For some Endpoint Encryption agents, a restart is required to complete the uninstallation.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Request timeout: agent uninstallation</td>
<td>The timeout period is 30 minutes. After a timeout, initiate a new uninstallation request.</td>
</tr>
</tbody>
</table>

### Note

Make sure that the endpoint meets the minimum system requirements before deploying Endpoint Encryption agents. Microsoft .Net Framework 2.0 SP1 or above is required. For information about system requirements, see the *Endpoint Encryption Installation and Migration Guide*. 
**Table E-4. Installation Error Codes**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Error Code</th>
<th>Problem and Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Encryption</td>
<td>1603</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>-3</td>
<td>The user name or password is invalid. Verify the credentials and try to log on to PolicyServer again.</td>
</tr>
<tr>
<td></td>
<td>-6</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td></td>
<td>-13</td>
<td>The endpoint does not meet the minimum system requirements. Upgrade the RAM or disk space and try to install the agent again.</td>
</tr>
<tr>
<td>Agent</td>
<td>Error Code</td>
<td>Problem and Resolution</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Management for Microsoft BitLocker</td>
<td>1603</td>
<td>Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.</td>
</tr>
<tr>
<td>-13</td>
<td></td>
<td>Unable to install the Endpoint Encryption agent. Microsoft BitLocker requires Trusted Platform Module (TPM). The endpoint either does not support TPM, TPM is not enabled in BIOS, or TPM is locked by another logged on user. Enable TPM in BIOS or contact the system administrator for assistance.</td>
</tr>
</tbody>
</table>
| -14                                        |            | Unable to install the Endpoint Encryption agent. The operating system is not supported. Install one of the following supported operating systems and then try again:  
- Windows 7 32-bit or 64-bit, Ultimate or Enterprise edition  
- Windows 8 32-bit or 64-bit, Professional or Enterprise edition |
| -15                                        |            | Full Disk Encryption is already installed.                                                                                                                |
| -16                                        |            | Unable to install the Endpoint Encryption agent. The endpoint is already encrypted.                                                                     |
Using OfficeScan to Uninstall Endpoint Encryption Agents

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem. This procedure explains how to uninstall Endpoint Encryption agents using the OfficeScan Endpoint Encryption Deployment Tool plug-in.

Procedure

1. Select the Endpoint Encryption device.

   **Note**
   To select multiple Endpoint Encryption devices, hold SHIFT and select applicable endpoints.

2. Click **Uninstall** and select the appropriate Endpoint Encryption agent from the drop-down list.

3. Click **OK** to confirm the deployment.

   The Endpoint Encryption agent uninstall command is deployed.

4. The Endpoint Encryption agent uninstallation is complete when OfficeScan displays the confirmation message.

   **Note**
   All future deployment commands fail if the Endpoint Encryption device is not restarted after the uninstall command is initiated and completes. If the uninstall cannot complete, follow the manual uninstallation process in the *Endpoint Encryption Installation and Migration Guide*.

When uninstallation completes, the Endpoint Encryption agent is removed and the product folder is deleted from the endpoint.
The following table explains the terminology used throughout the Endpoint Encryption documentation.

**Table F-1. Endpoint Encryption Terminology**

<table>
<thead>
<tr>
<th><strong>TERM</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Software installed on an endpoint that communicates with a management server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of identifying a user.</td>
</tr>
<tr>
<td>ColorCode™</td>
<td>The authentication method requiring a color-sequence password.</td>
</tr>
<tr>
<td>Command Line Helper</td>
<td>A Trend Micro tool for creating encrypted values to secure credentials when creating Endpoint Encryption agent installation scripts.</td>
</tr>
<tr>
<td>Command Line Installer Helper</td>
<td>A Trend Micro tool for creating encrypted values to secure credentials when creating Endpoint Encryption agent installation scripts.</td>
</tr>
<tr>
<td>Control Manager</td>
<td>Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels.</td>
</tr>
<tr>
<td><strong>TERM</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain authentication</td>
<td>The authentication method for single sign-on (SSO) using Active Directory.</td>
</tr>
<tr>
<td>DriveTrust™</td>
<td>Hardware-based encryption technology by Seagate™.</td>
</tr>
<tr>
<td>Encryption Management for Microsoft BitLocker</td>
<td>The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint. Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. For more information, see <em>About Full Disk Encryption on page 14-2</em>.</td>
</tr>
<tr>
<td>Encryption Management for Apple FileVault</td>
<td>The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. For more information, see <em>About Full Disk Encryption on page 14-2</em>.</td>
</tr>
<tr>
<td>Endpoint Encryption Device</td>
<td>Any computer, laptop, or removal media (external drive, USB drive) managed by Endpoint Encryption.</td>
</tr>
<tr>
<td>Endpoint Encryption Service</td>
<td>The PolicyServer service that securely manages all Endpoint Encryption 5.0 agent communication. For more information, see <em>About PolicyServer on page 1-10</em>. For Endpoint Encryption 3.1.3 and below agent communication, see Legacy Web Service.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured when installing PolicyServer. One PolicyServer database may have multiple Enterprise configurations. However, Endpoint Encryption configurations using Control Manager may only have one Enterprise.</td>
</tr>
<tr>
<td><strong>TERM</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Encryption</td>
<td>The Endpoint Encryption agent for file and folder encryption on local drives and removable media. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. For more information, see <em>About File Encryption on page 13-2</em>.</td>
</tr>
<tr>
<td>Fixed password</td>
<td>The authentication method for using a standard user password consisting of letters and/or numbers and/or special characters.</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>The Endpoint Encryption agent for hardware and software encryption with preboot authentication.</td>
</tr>
<tr>
<td>KeyArmor</td>
<td>The Endpoint Encryption password-protected, encrypted USB device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td><strong>Endpoint Encryption 5.0 does not have KeyArmor devices. However, legacy KeyArmor devices are supported.</strong></td>
</tr>
<tr>
<td>Legacy Web Service</td>
<td>The PolicyServer service that securely manages all Endpoint Encryption 3.1.3 and below agent communication. For details, see <em>About PolicyServer on page 1-10</em>. For Endpoint Encryption 5.0 communication, see Endpoint Encryption Service.</td>
</tr>
</tbody>
</table>

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPAL</td>
<td>Trusted Computing Group’s Security Subsystem Class for client devices.</td>
</tr>
<tr>
<td>Password</td>
<td>Any type of authentication data used in combination with a user name, such as fixed, PIN, and ColorCode.</td>
</tr>
<tr>
<td>PIN</td>
<td>The authentication method for using a Personal Identification Number, commonly used for ATM transactions.</td>
</tr>
<tr>
<td>PolicyServer</td>
<td>The central management server that deploys encryption and authentication policies to the Endpoint Encryption agents.</td>
</tr>
<tr>
<td>Remote Help</td>
<td>The authentication method for helping Endpoint Encryption users who forget their credentials or Endpoint Encryption devices that have not synchronized policies within a predetermined amount of time.</td>
</tr>
<tr>
<td>Recovery Console</td>
<td>The Full Disk Encryption interface to recover Endpoint Encryption devices in the event of primary operating system failure, troubleshoot network issues, and manage users, policies, and logs.</td>
</tr>
<tr>
<td>Repair CD</td>
<td>The Full Disk Encryption bootable CD that can decrypt a drive before removing Full Disk Encryption in the event that the disk becomes corrupted.</td>
</tr>
<tr>
<td><strong>TERM</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RESTful</td>
<td>Representational State Transfer web API. The AES-GCM encrypted communications protocol used by Endpoint Encryption 5.0 agents. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Without authentication, the service denies all policy transactions.</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>A mechanism for performing two-factor authentication for a user to a network resource.</td>
</tr>
<tr>
<td>SED</td>
<td>Secure Encrypted Device. A hard drive, or other device, which is encrypted.</td>
</tr>
<tr>
<td>Self Help</td>
<td>The authentication method for helping Endpoint Encryption users provide answers to security questions instead of contacting Technical Support for password assistance.</td>
</tr>
<tr>
<td>Smart card</td>
<td>The authentication method requiring a physical card in conjunction with a PIN or fixed password.</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol. The encrypted communications protocol used by all Endpoint Encryption 3.1.3 and older agents to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts.</td>
</tr>
</tbody>
</table>
Index

Symbols
"Log on as batch job" policy, A-64

A
about
account types, 2-5
authentication, 2-1
client-server architecture, 1-7
Control Manager integration, 3-2
Encryption Management for Apple
FileVault, 15-10
Encryption Management for Microsoft
BitLocker, 15-4
Endpoint Encryption, 1-2
Endpoint Encryption Service, 1-10
File Encryption, 13-1, 13-2
FIPS, 1-7
Full Disk Encryption
   Encryption Management for
   Apple FileVault, 14-2
   Encryption Management for
   Microsoft BitLocker, 14-2
groups, 8-5
Legacy Web Service, 1-10
Maintenance Agreement, 17-2
OfficeScan, E-2
PolicyServer, 1-10, 3-1, 8-1
PolicyServer MMC, 8-2
users, 8-5
widgets, 4-4
Accessibility
   on-screen keyboard, 14-7
accounts
types, 2-5

Active Directory, 1-7, 2-9, 6-11, 11-19
   import users, 6-7, 11-6
   resetting password, 6-14, 11-22
agents, 1-14
   services, E-12
agent tree, E-5
   about, E-5
   specific tasks, E-5
alerts, 16-12
appendices, 1
authentication, 1-2
   about, 2-1
   account types, 2-5
   change method, 14-8
   changing password, 13-6
   ColorCode, 2-6, 2-8, 13-5, 14-10, 14-11
   domain, 2-9
   domain authentication, 2-6
   File Encryption, 13-2
   fixed password, 2-6, 2-10
   Full Disk Encryption, 14-3
   LDAP, 2-9
   options, 2-7
   PIN, 2-6, 2-11, 13-6
   prerequisites, 2-9
   remote help, 11-30, 14-13
   Remote Help, 2-6, 2-11, 14-13
   security options, 2-2, 13-8
   Self Help, 2-6, 2-12, 11-26, 14-15, 14-17
      answers, 14-17
   setup requirements, 2-9
   single sign-on, 13-3
   smart card, 2-13, 11-23, 11-24, 13-4, 14-14
   authentication methods, 2-6
automatic deployment settings
  Scheduled Download, A-59

B
burning discs, 13-18

C
centrally managed, 5-23
central management, 1-2
changing passwords, 14-9
changing setting permissions, 5-22
client-server architecture, 1-7
ColorCode, 2-8, 14-10
Command Line Helper, 14-2, 14-41
Command Line Helper Installer, 14-2
community, 17-6
components
downloading, A-38
configuring, A-56
  managed products, A-24
  Scheduled Download
    automatic deployment settings, A-59
  Scheduled Download Exceptions, A-48
  Scheduled Download Settings, A-57
user accounts, A-9
configuring proxy settings
managed server list, 5-30
Control Manager, 1-14, 3-2, 3-4, A-1, A-6
  about, 1-14, 3-2, A-1
  accounts, A-9
  agent, 3-5, A-7
  antivirus and content security components, A-39, A-40
  basic features, A-3
  configuring accounts, A-9
  features, A-3
  mail server, 3-4, A-6
  managed product, A-15
  MCP, 3-5, A-7
  policies, 5-1
  report server, 3-4, A-6
  SQL database, 3-4, A-6
  Trend Micro Management Infrastructure, 3-5, A-7
users
  add to policy, 6-21
  remove from policy, 6-23
web-based management console, 3-5, A-7
web server, 3-4, A-6
widget framework, 3-6, A-8

Control Manager antivirus and content security components
  Anti-spam rules, A-39
  Engines, A-39
  Pattern files/Cleanup templates, A-39
copying policy settings, 5-23
creating
folders, A-35
creating policies
centrally managed, 5-23
copying settings, 5-23
setting permissions, 5-22

CSV, 11-5

D
DAAutoLogin, 14-2, 14-41
dashboard
  using, 4-2
data protection, 1-2
data recovery, 14-35
data views
  understand, A-67
Decrypt Disk, 14-23
decryption
  Recovery Console, 14-23
deleting
tabs, 4-4
deleting policies, 5-25
demilitarized zone, 14-18
deployment
  OfficeScan, E-9–E-11
deployment plans, A-60
device, 1-2
devices, 2-2, 4-11, 7-1, 7-7, 12-1
  add to group, 10-11, 12-3
  add to policy, 7-3
  directory listing, 12-11
  finding, 7-9
  group membership, 12-11
  kill command, 2-4, 7-14, 12-12
  lock, 3-22, 5-20
  locking, 2-4, 7-15, 12-12
  reboot, 2-4, 7-15, 12-13
  recovery key, 2-4, 7-10, 12-7
  remove, 7-16, 12-5
  remove Enterprise device, 7-16, 12-5
  remove from group, 10-12, 12-4
  remove from policy, 7-6
  software token, 2-4, 7-9, 12-6
  view attributes, 7-11, 12-8
  Directory Management options, A-34
  Directory Manager, A-33
domain authentication, 2-9, 13-4
  File Encryption, 13-3
Download Center, 17-5
download components
  manually, A-41
downloading and deploying components, A-38
draft policies, 5-4

E
editing managed servers, 5-30
editing policies, 5-24, 6-21, 6-23
encryption, 1-6, 9-26
  archiving, 13-18
  digital certificate, 13-17
  features, 1-2
  file and folder, 13-2
  file encryption, 13-1
  File Encryption
    archive and burn, 13-14
  FIPS, 1-7
  fixed password key, 13-16
  full disk, 14-2
  hardware-based, 1-6, 14-2
  keys
    shared, 13-15
    local key, 13-14
    self-extracting, 13-16
    software-based, 1-6, 14-2
Encryption Management for Apple
FileVault
  about, 15-10
Encryption Management for Microsoft
BitLocker
  about, 15-4
  agent service, E-12
Endpoint Encryption
  about, 1-2
  tools, 14-2
error messages
  authentication, 2-2, 13-8
F
features, A-3
File Encryption, 13-1
agent service, E-12
archive, 13-14
archive and burn, 13-14, 13-18
authentication, 13-2
  ColorCode, 13-5
  domain, 13-3
  first-time, 13-2
  PIN, 13-6
  smart card, 13-4
burn archive with certificate, 13-19
burn archive with fixed password, 13-18
change PolicyServer, 13-12
changing password, 13-6
changing PolicyServer, 13-12
digital certificate, 13-17
  creating, 13-17
encryption, 13-14
file encryption, 13-2
first-time use, 13-2
fixed password key
  creating, 13-16
local key, 13-14, 13-15
PolicyServer sync, 13-10
Remote Help, 11-30, 13-7
reset password, 13-7, 13-10
secure delete, 13-19
shared key, 13-15
  creating, 13-16
single sign-on, 13-3
smart cards, 13-5
syncing with PolicyServer, 13-11
sync offline files, 13-12
tray icon
about, 13-10
unlock device, 11-30, 13-7
filtered policies, 5-4
reordering, 5-4
FIPS
  about, 1-7
  FIPS 140-2, 1-7
  security levels, 1-7
fixed password, 2-10
folders
  creating, A-35
  renaming, A-36
Full Disk Encryption, 14-1
agent service, E-12
authentication, 2-12, 14-15
  changing password, 14-9
  change, 14-23, 14-31
  change PolicyServer, 14-22
  changing enterprises, 14-29
clean up files, 14-40
connectivity, 14-17
Decrypt Disk, 14-23
menu options, 14-4
network configuration, 14-29
Network Setup, 14-29
patching, 14-42
PolicyServer settings, 14-17
port settings, 14-17
Recovery Console, 14-21
  manage policies, 14-28
  manage users, 14-26
  Windows, 14-22
recovery methods, 14-32
Remote Help, 11-30, 14-13
Self Help, 14-16
synchronize policies, 14-19
TCP/IP access, 14-17
  tools, 14-2
  uninstall, 14-32
Windows patches, 14-41
Full Disk Encryption Preboot, 14-3
  authentication, 14-8
  keyboard layout, 14-8
  menu options, 14-4
  network connectivity, 14-5
  on-screen keyboard, 14-7
  wireless connection, 14-5

G
  groups, 8-5, 10-1
    creating offline groups, 10-13
    install to group, 11-16
    modifying, 10-5
    offline groups, 10-12
    remove device, 10-12, 12-4
    removing, 10-5
    subgroups, 10-2
    types, 10-2

H
  help desk policies, 11-29

I
  importing users, 11-5

K
  key features, 1-2

L
  LDAP, 2-9
  LDAP Proxy, 6-4, 11-3
  log events, 16-11
  logs, 14-28, 16-1, A-65
    alerts, 16-12
    managing events, 16-11
    querying, A-67
    setting alerts, 16-12

M
  maintenance, 16-2
  Maintenance Agreement
    about, 17-2
    expiration, 17-2
    renewal, 17-2
  managed products
    configuring, A-24
    issue tasks, A-25
    recovering, A-30
    renaming, A-36
    searching for, A-31
    viewing logs, A-26
  managed server list, 5-26
    configuring proxy settings, 5-30
    editing servers, 5-30
  manually download components, A-41
  MBR
    replacing, 14-25
  MCP, 3-5, A-7
    modifying
      tabs, 4-3

N
  Network Setup, 14-29

O
  OfficeScan
    uninstalling agents, E-17
  online
    community, 17-6
    on-screen keyboard, 14-7
passwords, 1-2, 6-11, 11-19
  change fixed password, 6-15
  change method, 6-15
Remote Help, 11-27
resetting, 6-11, 6-12, 11-21
  Active Directory, 11-22
  Enterprise Administrator, 11-20
  Enterprise Authenticator, 11-20
  Group Administrator, 11-21
  Group Authenticator, 11-21
  user, 11-21, 11-22
resetting active directory, 6-14
resetting Enterprise Administrator/ Authenticator, 6-11
resetting fixed password, 6-13
resetting Policy Administrator/ Authenticator, 6-12
resetting to fixed password, 11-22
resetting user, 6-13, 6-14
Self Help, 11-26
pending targets, 5-8
Personal Identification Number (PIN), 2-11
Plug-in Manager, E-3
policies, 1-2, 5-12
  allow user recovery, 14-21
  common, 3-19, 5-17, 9-30
    agent, 9-30
    authentication, 9-30
  deleting, 5-25
  editing, 5-24, 6-21, 6-23
File Encryption, 3-17, 5-15
  computer, 9-26
  encryption, 9-26
  login, 9-28
  password, 9-29
Full Disk Encryption, 3-15, 5-13, 9-19,
  9-26, 14-19
    client, 9-19
    encryption, 9-20
    login, 9-20
    password, 9-25
  indicators, 8-15, 9-2
  policy mapping, D-1
PolicyServer, 9-14
  Administrator, 9-15
  Authenticator, 9-16
  console, 9-14
  log alerts, 9-17
  service pack download, 9-18
  welcome message, 9-18
remove device, 7-6
Support Info, 11-29
synchronization, 14-2
synchronizing, 14-19
user, 3-14, 5-12
policy
  install devices, 6-19
  policy control, 13-1
  policy list, 5-4, 5-6
  policy management, 5-2
    centrally managed, 5-23
    copying policy settings, 5-23
    deleting policies, 5-25
    draft policies, 5-4
    editing managed servers, 5-30
    editing policies, 5-24, 6-21, 6-23
    filtered policies, 5-4
    managed server list, 5-26
    pending targets, 5-8
    policy list, 5-4, 5-6
    policy priority, 5-4, 5-7
reordering policies, 5-4
setting permissions, 5-22
specified policies, 5-4
targets, 5-7
understanding, 5-2
upgrading policy templates, 5-31

policy mapping
  Control Manager, D-1
  PolicyServer, D-1

policy priority, 5-7

PolicyServer
  advanced premise, 16-15
  client web service, 1-7
  enabling applications, 8-19
  enhancements, 1-3
  getting started, 3-1, 8-1
  interface, 8-4
  log events, 16-11
  logs, 16-1
  maintenance, 16-2
  MMC hierarchy, 8-4
  MMC window, 9-4
  policies, 5-6, 9-1, 9-2, 9-4
    editing, 9-4
    Support Info, 11-29
  relay SMS/email delivery, 16-13
  Remote Help, 11-27
  reports, 16-1, 16-15
  setting log alerts, 16-12
  smart card, 11-24
  subgroups, 10-4
  Support Info, 11-29

PolicyServer MMC, 1-7
  add enterprise user, 8-10, 11-3
  add top group, 8-6, 10-3
  authentication, 8-2

fields and buttons, 8-16, 9-3
first time use, 8-2
groups, 8-5
  adding users, 8-8, 10-5, 11-11
modifying policies, 8-17
offline groups, 10-12
  creating, 10-13
  updating, 10-15
policies, 8-15
  editing
    multiple choice, 9-8
    multiple option, 9-12
    policies with ranges, 9-4
    text string, 9-11
    True/False, Yes/No, 9-6
users, 8-5
  add enterprise user, 8-8, 10-5, 11-11
  add to group, 8-8, 8-13, 10-5, 10-8,
    11-11, 11-13
users and groups, 8-6

policy settings
  copying, 5-23
policy targets, 5-7
policy templates, 5-31
policy types
  draft, 5-4
  filtered, 5-4
  policy priority, 5-7
  specified, 5-4
product components, 1-7
product definitions, F-1
Product Directory
  deploying components, A-22
product overview, 1
proxy settings
  managed server list, 5-30
Q
query logs, A-67

R
recovering
managed products, A-30
recovery
clean up files, 14-40
recovery console
logon, 14-22
Recovery Console, 14-20
access, 14-21
Windows, 14-22
changing enterprises, 14-29
changing PolicyServer, 14-23, 14-31
Decrypt Disk, 14-23
functions, 14-20
log on, 14-21
manage policies, 14-28
manage users, 14-26
Mount Partitions, 14-25
network configuration, 14-29
Network Setup, 14-29
recovery methods, 14-32
Repair CD, 14-36
Restore Boot, 14-25
users
add, 14-27
delete, 14-28
edit, 14-26
view logs, 14-28
recovery methods, 14-32
registering
to Control Manager, A-8
registration
key, 17-2
profile, 17-2

URL, 17-2
Remote Help, 2-2, 2-4, 2-11, 6-11, 7-15, 11-19,
11-27, 12-12, 13-8, 14-13
renaming
folders, A-36
managed products, A-36
Repair CD, 14-2, 14-32, 14-34
data recovery, 14-35
decryption, 14-36
reporting, 1-2
reports, 16-1, 16-15
alert, 16-19
display errors, 16-21
displaying reports, 16-20
icons, 16-16
one-time reports, A-82
options, 16-16
scheduled reports, 16-20, A-88
standard, 16-17, 16-18
templates, A-69
types of, 16-17
report templates, A-69
Restore Boot, 14-25

S
schedule bar, A-12
Scheduled Download
configuring
automatic deployment settings,
A-59
Scheduled Download Exceptions
configuring, A-48
Scheduled Download Frequency
configuring, A-56
Scheduled Downloads, A-49
Scheduled Download Schedule
configuring, A-56
Scheduled Download Schedule and Frequency, A-56
Scheduled Download Settings
configuring settings, A-57
searching
managed products, A-31
security
account lock, 2-11, 14-13
account lockout action, 2-11, 14-13
account lockout period, 2-11, 14-13
anti-malware/antivirus protection, 1-2
device lock, 2-11, 14-13
erase device, 2-2, 13-8
failed login attempts allowed, 2-11, 14-13
remote authentication required, 2-2, 13-8
time delay, 2-2, 13-8
Self Help, 2-12, 6-11, 11-19, 14-15
answers, 14-17
defining answers, 14-16
password support, 11-26
setting permissions, 5-22
showing permissions, 5-22
smart card, 2-13, 11-23, 14-14
authentication, 11-24
smart cards, 2-13, 11-23, 14-14
specified policies, 5-4
priority, 5-4
SSO, 2-9
summary dashboard, 4-1
adding tabs, 4-3
deleting tabs, 4-4
modifying tabs, 4-3
tabs, 4-2
support
knowledge base, 17-6
resolve issues faster, 17-8
TrendLabs, 17-9
synchronization
File Encryption, 13-11
T
tabs
about, 4-2
deleting, 4-4
modifying, 4-3
summary dashboard, 4-2
targets, 5-7
pending, 5-8
terminology, F-1
tokens, 11-24, 11-26, 14-15
tools
Command Line Helper, 14-41
DAAutoLogin, 14-41
Recovery Console, 14-29
Repair CD, 14-34
top group, 8-6, 10-3
TrendLabs, 17-9
Trend Micro Control Manager
managed product user access, A-11
registering to, A-8
trial license, 17-3
U
understand
data views, A-67
deployment plans, A-60
log queries, A-67
logs, A-65
understanding
Endpoint Encryption, 1-1
uninstalling
agents, E-17
upgrading policy templates, 5-31
URLs
   registration, 17-2
users, 2-4, 6-1, 8-5, 11-1
   Active Directory passwords, 11-22
   adding, 6-4, 11-3
   adding existing user to group, 8-13, 10-8, 11-13
   adding existing user to policy, 6-21
   adding new user to group, 8-8, 10-5, 11-11
   add new enterprise user, 8-10, 11-3
   change default group, 11-15
   change default policy, 6-20
   finding, 11-8
   group membership, 11-10
   group vs enterprise changes, 11-9
   import from AD, 6-7, 11-6
   importing with CSV, 11-5
   install to group, 11-16
   install to policy, 6-19
   lockout, 3-22, 5-20
   modifying, 11-9
   passwords, 6-11, 11-19
   policy membership, 6-16
   remove from group, 10-10, 11-18
   remove user from policy, 6-23
   restore deleted, 6-25, 11-18, 16-10
users and groups, 8-6

V
   viewing
      managed products logs, A-26

W
   widgets
      adding, 4-6
      adding tabs, 4-3
      configuring, 4-7
   customizing, 4-6
deleting, 4-8
description, 4-8
Endpoint Encryption, 4-8
Endpoint Encryption Device Lockout, 4-19
Endpoint Encryption Security
   Violations Report, 4-22
Endpoint Encryption Status, 4-13
Endpoint Encryption Unsuccessful
   Device Logon, 4-16
   User Logon, 4-18
   options, 4-7
   understanding, 4-4
Windows patch management, 14-41